RCMP
ROYAL CANADIAN MOUNTED POLICE

SERVING THE POLICE COMMUNITY SINCE 1939

GAZETTE

VOL.75, NO. 3, 2013

NEW TECHNOLOGY
PALM PRINTS DATABASE HELPS CONNECT CASES P. 34

FOLLOW THE MONEY
EXAMINING FRAUD AND FINANCIAL CRIMES

CORPORATE CORRUPTION
FINANCIAL INTEGRITY UNITS TARGET FOREIGN BRIBERY P.7

AFFINITY FRAUD
WHEN 'FRIENDS' CAN'T BE TRUSTED P.22

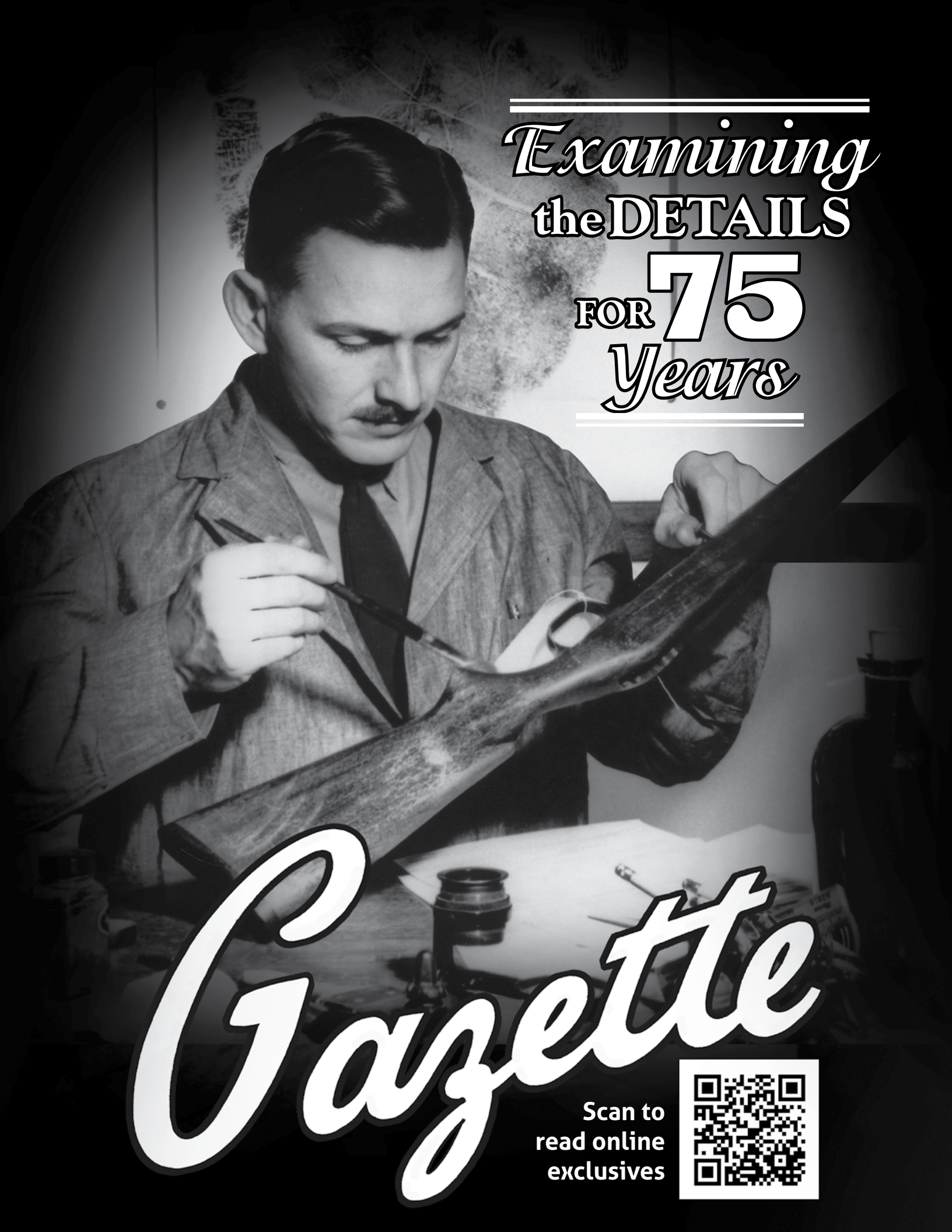
FINANCIAL INTELLIGENCE
INTEGRATED UNIT SUPPORTS INVESTIGATIONS P.11

FATIGUE AND SHIFT WORK
SMALL CHANGES CAN IMPROVE SAFETY P.26

RCMP-GRC.GC.CA

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada


Examining
the DETAILS
FOR 75
Years
Gazette
Scan to
read online
exclusives

GAZETTE
Serving the police community since 1939
Vol. 75, No. 3, 2013
A Royal Canadian Mounted Police Publication

COVER SECTION

DEPARTMENTS

FINANCIAL CRIME IS NO TRIVIAL MATTER

Canadians work hard for their money. They want to have confidence that their earnings are safe from fraud, theft or abuse. They also want to know that those who commit financial crimes — be they lone scammers or organized crime groups — don't get away with it.

In our cover section, we look at fraud and financial crime in Canada, and the RCMP's involvement in bringing those who commit these crimes to justice.

Mallory Procunier examines corruption in international business, a practice in which corporations offer gifts and cash to foreign officials to gain a business advantage. For many years, it was the norm. But two recent high-profile investigations by the RCMP's financial integrity units are making Canadian companies think twice about engaging in foreign bribery.

Sigrid Forberg writes about the expertise of financial crime investigators. While these officers need to know their way around a calculator, they must also rely on traditional policing skills and tools to follow the paper trail. As her article explains, persistence is important, as that trail often crosses national and international boundaries.

White-collar criminals in Quebec have a new foe in the Joint Securities Intelligence Unit, comprising members of Quebec's Autorité de marchés financiers, the Sûreté du Québec and the RCMP. This collaborative approach ensures that information critical to an investigation is quickly identified and shared with those who need to know.

We also hear from several agencies on their fight against fraud and scams.

The Toronto Police Service teamed up with the Financial Services Commission of Ontario to tap into social media for fraud prevention. They started fraud chat, a weekly Twitter chat on fraud and financial crime topics, and now reach more than 700,000 people each week.

In the United Kingdom, the National Fraud Intelligence Bureau provides a simple, victim-focused service so that citizens can report fraud by telephone or online. The reports help to feed the bureau's KnowFraud database and allow police across the country to identify trends and connect the dots.

The Minnesota Bureau of Criminal Apprehension uncovered a sophisticated system of identity theft, bank fraud and money laundering involving more than 8,700 victims across the globe. Learn about the extraordinary co-operation and tracking system that allowed police to identify and charge those involved.

And if you've ever wondered how fraudsters get victims to part with their money, read Frank Perri's article on affinity fraud. These offenders target members of religious institutions and cultural groups. And when they offer financial tips, their peers listen — and get taken.

While these crimes are less eye-catching than shootings or disasters, they are no trivial matter. Canadians and victims everywhere would likely agree. ■

— Katherine Aldred

ON THE COVER: *Financial crime investigations often take investigators out of the office and into the field, where they have to rely on traditional policing skills. Photo: RCMP*

GAZETTE

PUBLISHER: Nancy Sample

EDITOR: Katherine Aldred

WRITERS: Sigrid Forberg, Mallory Procunier

WEB PUBLISHER: Richard Vieira

GRAPHIC DESIGN: Lisa McDonald-Bourg

ADMINISTRATIVE SUPPORT AND CIRCULATION: Bernard Rice

TRANSLATION: RCMP Translation Services

PRINTING: Performance Printing

The *Gazette* (ISSN 1196-6513) is published in English and French by the National Communication Services of the Royal Canadian Mounted Police in Ottawa. The views expressed in any material published in the magazine or in its online version are those of the authors and do not necessarily reflect the official opinion of the Royal Canadian Mounted Police. Canada Post Publications Mail Agreement 40064068. The *Gazette* is published four (4) times a year and is issued free of charge on a limited basis to accredited police forces and agencies within the criminal justice system. Personal subscriptions are not available.

The *Gazette* welcomes contributions, letters, articles and comments in either official language. We reserve the right to edit for length, content and clarity.

HOW TO REACH US:

RCMP *Gazette*
73 Leikin Drive,
M-8 Building, 1st Floor, Room 801
Ottawa, ON K1A 0R2
CANADA

Phone: 613-843-4570
E-mail: gazette@rcmp-grc.gc.ca
Internet: www.rcmp-grc.gc.ca/gazette

STAY CONNECTED WITH THE RCMP

Visit our website:
www.rcmp-grc.gc.ca

Follow us on Facebook:
www.facebook.com/rcmpgrc

Follow us on Twitter:
@rcmpgrcpolice #rcmpgazette

Watch us on YouTube:
www.youtube.com/rcmpgrcpolice

Subscribe to RSS updates:
www.rcmp-grc.gc.ca/rss/index-eng.htm

BARWATCH SHOWS BENEFITS

The Ridge Meadows RCMP detachment is working towards making its local bars safer.

The detachment, which serves both Maple Ridge and Pitt Meadows in the Lower Mainland of British Columbia, renewed its BarWatch program in April 2011.

For the last two years, local police met quarterly with bar and restaurant owners in the two communities to provide a forum for the businesses to have real conversations about public safety issues.

Insp. David Fleugel, the operations officer for Maple Ridge, says while gang activity is one of those issues, so are fire safety and alcohol ordinances. He adds the meetings offer both sides an opportunity to discuss growing concerns or troubling trends in a more casual setting.

"We want to make sure that we actually have a meaningful dialogue before any enforcement happens," says Fleugel. "We don't want to just walk in handing out tickets."

Fleugel says part of the success is attributed to both city mayors and local and provincial politicians that have been very supportive, recognizing the value and benefits of the BarWatch program.

"Working from the inside rather than just legislating something is by far the best approach in my view," says Ernie Daykin, the mayor of Maple Ridge. "We want our bars to be successful, but also responsible. And by working together, I think they have made a difference."

One of the most important aspects of the program to Fleugel is that the BarWatch committee is always chaired by a local business owner. He says this helps show that it's not a police-mandated addition to their workload, but a mutually beneficial discussion.

The BarWatch program currently has about 50 per cent participation, but is using educational forums and personal invitations from detachment management to encourage the rest of the businesses to join as well. Fleugel says the united front helps show the public that their safety is a top priority.

"I think it sends a really strong message of partnership, which is one of the keys to success in policing," says Fleugel. "We need to demonstrate to the community that we're working together to solve the problems before they become bigger problems and I think that's what this does." ■

— Sigrid Forberg

NEW UNIT CLOSES DOOR ON BREAK AND ENTERS

In response to a 100 per cent increase in residential break-ins during December 2012 and January 2013, the Burnaby detachment in British Columbia struck up a temporary task force that put break and enters (B&E) at the front and center of its operations. And the approach is stopping thieves in their tracks.

The detachment seconded members from various sections to focus on investigating this type of crime and getting those responsible off the street.

Between February and March 2013, the task force oversaw every B&E case in Burnaby, located east of Vancouver. That way, members could become familiar with the cases and were easily able to figure out if several B&Es were perpetrated by the same individual.

This type of task force also ensured that investigations never became stagnant since members worked continuously to quickly gather evidence and push charges forward to Crown counsel.

"We were able to take people off the street pretty quickly and that allowed us to disrupt a lot of crime patterns that we saw emerge throughout the late fall and into December," says S/Sgt. Andy LeClair, who led the B&E task force.

In its first few weeks, the task force worked with other agencies to target key offenders in the city and put many of them behind bars. Between January and February 2013, the number of residential B&Es per month dropped from 126 to 55.

RCMP

The Burnaby task force drew a lot of public attention for how quickly it curbed the city's B&E problem.

The task force also took a proactive approach to Burnaby's B&E problem. LeClair explains that the most common type in the area is the knock-and-see B&E, where a perpetrator knocks on a door to see if anyone is home. If no one answers the door, he or she breaks in.

To educate the public, members of the task force actively canvassed hard-hit neighbourhoods and told the public to keep an eye out for anything out of the ordinary. "Realistically, from a preventative standpoint, a heads-up citizen is key," LeClair says.

He says that a temporary task force is a common way to deal with a spike in any crime, whether it's street-level cellphone robberies or residential B&Es. A task force isolates the problem faster and usually operates until the problem is under control. ■

— Mallory Procunier

COURSE IN THAILAND OPENS EYES FOR MEMBER

Earlier this year, Cst. John Lamming travelled to Bangkok, Thailand, with 16 other individuals from across the world for a three-month course on peace and conflict resolution sponsored by Rotary International.

Lamming, a member of the RCMP Combined Forces Special Enforcement Unit in Grande Prairie, Alta., was one of three police officers in the group and the only one representing a Canadian force.

With a master's degree in history, Lamming brings an academic perspective to his police work. Having prepared a conflict analysis on organized crime in his community while he was away, in the short time since his return, Lamming has been looking at what he can do to implement his plan and deter individuals from crime as well as catch and charge offenders.

The group also travelled to Nepal, where Lamming says he gained important perspective about some of the challenges countries with less reformed security sectors face.

"I would like to think that my world view is pretty well-rounded and that I had a good idea of how things are but until you go and you see it and you experience it, you almost can't understand it," says Lamming. "To see it just kind of opens up your eyes."

Cst. John Lamming

Cst. John Lamming (centre) travelled to Thailand to participate in a peace and conflict resolution course, which he's now applying to his work in Grande Prairie, Alta.

Since his return, Lamming has been presenting what he's learned at the local Rotary meeting and at a youth conference about peace in Edmonton, Alta., in May.

Jane Manning, a member of one of the local Rotary International chapters in Grande Prairie, was the one who originally suggested Lamming apply for the course. Manning says she's always been impressed with Lamming's thoughtful and studious personality and after seeing his application, knew that he was a perfect fit for the course.

"I hadn't really thought until we got talking about how applicable it is to some of the work he does now with members and people in our community," says Manning. "It was interesting to see how you can apply conflict resolution at a personal level as opposed to just on a big world peace level." ■

— Sigrid Forberg

PHONY FIREARMS

Police in Kelowna, British Columbia are asking the public to help curb sightings of fake firearms in the area.

Over the past year and a half, the RCMP detachment in Kelowna has had a boost in calls from people claiming to have seen others carrying guns in public.

"I've certainly seen, time and again, where people are wandering out and about, they've got a replica gun down the back of their pants or they're carrying it and people are going to call us because that's out of the norm," says Cst. Kris Clark of the Kelowna detachment.

Clark says the danger of replica guns lies in not being able to tell whether they're real or not. Replica guns are often built to look like the real thing, and police officers can't usually tell the difference until they see them up close.

"We don't have the luxury of examining a weapon before engaging our own," Clark says. "We have to rely on our knowledge, experience and perceptions in order to respond, but when faced with an apparent threat of a firearm, the results could be disastrous."

To try and curb the problem, detachment members have been speaking to the public about safe ways to transport a firearm, such as in a locked case, whether it's real or not. Members also want youth to understand that they are creating fear in members of the public by carrying a replica gun.

Clark says the best advice for any police officer is to treat every gun like a real gun. "Respond properly and use your training and tactical skills to conduct a safe arrest and once the subject's under control, that's when you can make the determination whether it's real or not," Clark elaborates.

He explains that the human body is built to respond to threats and a gun can bring on auditory, visual and heart rate changes. "All these physiological changes make it that much more difficult to make a determination when you're in that situation so you need to be safe, get the subject under control, make the scene safe, and then see if the gun is real or not," Clark says. ■

— Mallory Procunier

Even police officers find it hard to tell the difference between a replica gun (left) and a real gun (right).

RCMP

An explosion at a natural gas well in Bangladesh prompted Calgary-based Niko Resources Inc. to bribe foreign officials to issue a smaller fine.

A LITTLE PAYMENT HERE, A LITTLE GIFT THERE

RCMP INVESTIGATORS TARGET CORRUPTION IN INTERNATIONAL BUSINESS

By Mallory Procunier

For many countries, conducting business on the basis of bribery is the norm. Corporations wishing to get ahead sometimes slip cash and expensive gifts to foreign officials to get what they want — a signature on a contract, usually. But since the RCMP landed several high-profile convictions on bribery cases that resulted in hefty fines, Canadian companies have been thinking twice about bending the rules while doing business abroad.

CORPORATE CORRUPTION

Bribery begins with a bit of extra cash. A company hires an "agent" in a foreign country to help connect it with local officials and to manage the logistics of doing business there, but it pays the agent a little too much money. The agent then passes the excess to a foreign official — usually someone in a high-ranking position in the federal government — to keep the transaction off the company's records.

For years, some Canadian companies quietly used these practices. But not only was this type of corruption giving certain companies an unfair advantage in the corporate playing field — it was also giving Canada the reputation of being too relaxed when it came to enforcing foreign bribery. Canada responded in 1998 with the creation of the *Corruption of Foreign Public Officials Act* (CFPOA), which gave law enforcement extra teeth to go after these types of white-collar criminals.

The RCMP took that responsibility in 2007 and created two international anti-corruption units (IACU) in Ottawa, Ont., and Calgary, Alta. These days, investigators with the RCMP's financial integrity teams handle these types of cases that can be forwarded by international policing agencies, corporate competitors, government agencies and others.

In fact, it was the Department of Foreign Affairs and International Trade (DFAIT) that led Calgary's IACU onto its first investigation under the CFPOA in 2009.

NEW TERRITORY

In 2005, there was a massive explosion at a natural gas well in Bangladesh that was owned and operated by Niko Resources Inc., a Calgary-based oil and gas company. Following the blast, villagers in the area surrounding the well protested that their drinking water had been contaminated and their crops devastated. Bangladesh's minister of energy and mineral resources was in charge of figuring out how much Niko should pay the villagers for the destruction it had caused.

Around that time, at its post in Dhaka, Bangladesh, DFAIT flagged a newspaper article to the RCMP that described how the

energy minister had received a $190,000 sport-utility vehicle (SUV) as a gift.

Having never investigated a potential bribery case before, the IACU was unsure how to begin. Cpl. Kevin Duggan, a former member of the IACU who now works for Calgary's financial integrity team, says that his unit began by collecting a multitude of financial information and company records about Niko before informing the company in 2009 that the RCMP was looking into its activities. At that point, Niko agreed to give the RCMP full access to its information.

"It was a relatively obscure process because we were all kind of figuring this out for the first time as to how we would wrap this up," Duggan says. "The good news was that their counsel at the time saw the potential ramifications of a conviction and what the fine could be."

The IACU conducted interviews in the United States, Barbados, Zimbabwe, Japan, the United Kingdom and Bangladesh. They even got co-operation from Switzerland — a country with notoriously difficult disclosure laws.

Through extensive and innovative investigation techniques that had never before been used by the IACU, investigators were able to find out that Niko's subsidiary in Bangladesh had purchased the SUV, and that it also paid for the minister to travel to both New York and Chicago to visit his family — all in an attempt to persuade the minister to lower the company's damages.

In June 2011, Niko pleaded guilty under the CFPOA and agreed to pay $9.5 million in fines and penalties.

With the help of the RCMP's financial integrity teams, bribery is becoming a less-common practice among Canadian companies.

WORKING TOGETHER

With one successful conviction under its belt, the IACU was earning the reputation of an effective investigative team that was committed to seeking penalties for and deterring future bribery and corruption among Canadian companies.

So when Griffiths Energy International Inc. (GEI) realized in 2011 that its books didn't line up — to the tune of $2 million — it chose to involve the IACU immediately.

"A company sometimes just finds out that it's made a mistake or one of its employees has made a mistake and it's decided to clear the slate," says S/Sgt. George Prouse of Calgary's financial integrity team.

The Toronto-based oil exploration and drilling company started up in 2009 when Brad Griffiths and his partners started looking at securing rights to drill at several oil blocks in Chad, Africa. After evaluating a few different ways of getting a production-sharing contract in the country, they decided that the best route would be to draw up a consulting agreement and sign a contract with the ambassador to Chad.

They quickly found out that, because the ambassador was a foreign public official, they couldn't hire him as a consultant. A few days later, the ambassador's wife formed her own corporation and entered into a $2-million consulting agreement with GEI. The company signed the contract, excluded the names of the partners involved and was eventually awarded the production-sharing contract in Chad.

"Griffiths Energy received this contract just as things were getting going for them," says Sgt. Donovan Fisher of Calgary's financial integrity team. "Brad Griffiths and his other partners had limited experience operating in the oil industry and no experience dealing with international production-sharing contracts."

Once the oil blocks were secure, Griffiths brought in new associates and set up a board of directors, which included business professionals who knew a thing or two about overseas oil drilling. But, several weeks later, Griffiths was killed in a boating accident in Ontario.

"We looked into that [death] as much as we could, but the best we could determine was that it was more of a bad coincidence than anything else," Fisher says.

Griffiths' board of directors were left with the company, so they began to look at setting up an initial public offering on the stock market.

"They did their due diligence and started going through the financial records and when they came upon the anomaly of $2 million that was paid to a consultant who turned out to be the ambassador's wife, they realized there was an issue," Fisher explains.

GEI immediately disclosed the payout to the RCMP and the public prosecution and asked for some time to do an internal investigation.

"On self-disclosures, we'll allow the

company to try and look into it themselves first and co-operate with us," Fisher says. "Griffiths was good at doing that."

While GEI was conducting a thorough investigation on their end, the IACU was busy checking open source materials, the Financial Transactions and Report Analysis Centre of Canada (FINTRAC) and liaising with foreign government officials to get the full picture.

"We had to ensure that they weren't just giving us one or two obvious things and hoping we'll just focus on that so that they could slide in anything else they've done under the radar," says Fisher. "On self-disclosures, we still try to conduct a fairly complete investigation on our own to ensure we've got the whole story."

In the end, GEI pleaded guilty to fraud on Jan. 22, 2013, and was fined $10.3 million for violating the CFPOA.

BEST PRACTICES

While investigating a CFPOA case, Prouse says that investigators must remember that, although the offence may be against a Canadian corporation, the case could be politically sensitive in the foreign jurisdiction where it occurred because it connects a prominent foreign official to bribery.

"Whether the country is known for bribery or not, they're still going to be protective of that and be sensitive to that so we have to make sure our investigators proceed in a very sensitive and politically correct manner so that we don't have that country shut down on us and not assist us in any way," Prouse says.

And just as a corporation needs to protect its brand, countries are now realizing that a corruption charge can leave a nasty mark on its reputation.

"Quite often, and we're finding it more and more, these countries are saying 'wait a minute, this corruption issue is on the world headlines and we want to get rid of it and work hard at getting rid of it,'" Prouse says.

Foreign bribery investigators sometimes rely on the pressure of the international community, which is looking to see how the country will handle allegations of corruption, to compel a diplomat to attend court or provide more information.

"That doesn't always give us exactly what we want, but at least it compels certain officials and countries to, on the face of it, co-operate with us," Fisher says. "At times, that's not the best-case scenario, but it still keeps things moving forward."

But when pressure alone doesn't work, it takes skill and a blend of experience and awareness to investigate a potential case of corruption. Prouse says that these types of investigators need to keep up on current events and understand the political and social climates of certain countries where corruption is likely to take place.

"We're operating in an intersection of politics, business and crime, and you have to be alive to do all three of them," Duggan says. "Every step you take, you have to weigh out not just legal consequences, but the political consequences as well. It adds a lot more layers to the process."

Fisher says that foreign law enforcement agencies and government departments can assist with this, and they can also provide more information for a case. Police liaison officers located in the target country are also great resources to be able to connect police with the right people and see the investigation from another perspective.

"IACU investigations are extremely sensitive and laden with implications affecting both Canadian international relations and the perception of law enforcement at home and abroad," says Sgt. Kelly Brophy, an RCMP police liaison officer with the Canadian High Commission in New Delhi, India. "For these reasons, special care and attention on the part of the IACU and the liaison officer is required to identify and mitigate issues, always with a view to complete thorough investigations."

SERIOUS IMPLICATIONS

Since GEI, Niko and several other sizeable bribery cases have been brought to a close by the RCMP, Canadian corporations are more serious than ever about creating strong compliance programs and assessing projects for corruption potential before they even begin.

"Companies have now seen what the threat is, they've seen the dollar signs attached to it and they've seen that their reputation will fall," Duggan says.

And by shaming these types of actions at home, investigators hope that Canadian companies will become ambassadors for change overseas.

"Once the majority of companies and businesses start taking a stand that they're not going to do it, the foreign countries that it's happening in are going to realize that it's not as easy to elicit a bribe out of a company coming in anymore and there's not going to be a lineup of other people who will pay the bribe," Fisher says. ■

NATIONAL APPROACH TO CORRUPTION

Offences that fall under the *Corruption of Foreign Public Officials Act* (CFPOA) are either brought to the attention of Calgary's financial integrity unit or the Sensitive and International Investigations Section of the RCMP in Ottawa's National Division.

In Ottawa, members of the division's former international anti-corruption unit (IACU) work among four teams of investigators who investigate the many corruption complaints they receive. Depending on the nature, impact and priority of a given complaint, a team of investigators is assigned a file to work on and carry forward.

Being so close to the seat of the federal government, Ottawa's unit is often called upon to deal with other sensitive cases that may have national and international political implications.

"Politically sensitive cases or financial crimes that are rooted in Canada with international connections would come to us," says Sgt. Patrice Poitevin, senior investigator and outreach co-ordinator for the Sensitive and International Investigations Section.

The section is currently involved in a number of ongoing investigations, such as the SNC Lavalin file, which has national and international implications.

— Mallory Procunier

CALCULATED CRIMES

INVESTIGATING OUTSIDE OF THE BOX

By Sigrid Forberg

Financial crime offenders can be as diverse as their crimes — often the only thing they might have in common is the impact their actions have on the integrity of Canada's economy.

And that's why it's important for police agencies to have knowledgeable and informed investigators when it comes to investigating financial crimes. In addition to the usual policing techniques and skills, investigators need to be interested in following the paper trail.

But that's not to say financial integrity cases revolve solely around bankers boxes and calculators. Whether it starts with a call from an international partner, or the local police, financial crime investigations often take investigators out of the office and into the field where they have to rely on their own personal and traditional policing skills.

INTERNATIONAL INVOLVEMENT

When German police came to the British Columbia's (B.C.) Department of Justice with an urgent mutual legal assistance treaty (MLAT) in November 2011, members of the RCMP's Financial Integrity Section in Victoria, B.C., rose to the occasion.

The German Federal Police had been investigating a hundred million euro ($124 million) Ponzi scheme with around 5,000 victims that led them to Canada's west coast and a suspect providing accounting services for an organized crime group. Within a short period of time, RCMP investigators tracked down the suspect and confirmed his identity.

Dealing with different time zones, the search warrant had to be executed at midnight local time to coincide with searches being conducted in Europe. Meanwhile, RCMP members questioned the suspect in a vacant unit in his apartment building while gathering evidence from his home and business addresses.

Cst. Dean Miller, the lead investigator on the file, was told by the German police that their search was one of the most successful. He says the case never could have been carried out so smoothly if it hadn't been for the members involved with varying and diverse skill sets.

"It's so important to have people who know what they're doing and are trained in their own specialized fields," says Miller. "Just having the right people in the right places made sure it was successful in the end."

Sgt. Andrew Cowan, the non-commissioned officer in charge of Federal, Serious and Organized Crime (Victoria), adds the success of the case also came down to the team's ability to work through certain investigational hurdles and tight timelines.

"I think this particular file was a good example of how flexible we can be," says Cowan. "We had to act quickly to bring resources and innovative solutions to a problem otherwise it would have seriously impacted our international policing partners."

Erwin Thomas Speckert was charged with possession of proceeds of crime, trafficking of proceeds of crime and money laundering after he was stopped at the Winnipeg bus terminal with $1.3 million in cash in a backpack.

RCMP

MUTUALLY BENEFICIAL

Security officials at the bus terminal in Winnipeg, Manitoba, were at a loss when they found $1.3 million in cash in the backpack of a man on his way to Vancouver, B.C. They called the city police, who then called in the RCMP to investigate from a proceeds of crime perspective.

Over the course of the investigation, they found connections to Ontario and British Columbia. Both those provinces had the individual on their radar as well. Because of the level of communication between the agencies, some information shared was able to jump-start or reinvigorate investigations elsewhere.

"It was real-time sharing of information between divisions," says Sgt. Pat Olson, with the RCMP in Manitoba's Financial Integrity Unit. "In that way it was excellent because there were so many parallel investigations going on."

Erwin Thomas Speckert is charged with the possession of proceeds of crime, trafficking of proceeds of crime and money laundering. The Toronto Combined Forces Special Enforcement Unit (CFSEU) has also charged Speckert's associate where the funds allegedly originated.

While the case is still ongoing, S/Sgt. Susan Riddell with Toronto CFSEU says working together has played an important part in the case so far.

"The collaborative effort of police agencies benefits all," says Riddell. "There is most often a financial crime aspect to organized crime investigations so it's important that organized crime investigators work in tandem with financial crime investigators."

While Olson says the fundamentals of all these cases are the same, there are still a few things that set financial crime investigations apart from other kinds of investigations.

"When you do a drug investigation, you're concerned with taking the drugs off the street. But the only way to really hurt them — it isn't just going to jail, it is also to take away what they've acquired illegally," says Olson. "It's a complete, full, true investigation."

PUTTING STOCK IN PARTNERSHIPS

RCMP FORMS JOINT INTELLIGENCE TEAM

By Sigrid Forberg

White-collar criminals in the province of Quebec have a new group of specialized investigators and analysts to contend with.

Comprised of two investigators, an analyst and a public servant from the RCMP and an investigator and analyst each from the Autorité de marchés financiers (AMF) and the Sûreté du Québec (SQ), the Joint Securities Intelligence Unit (JSIU) is an equal partnership between the three agencies created to combat economic crimes in Quebec.

The Joint Securities Intelligence Unit is responsible for gathering intelligence to help further financial crime investigations in Quebec, many of which are linked to the Montreal Stock Exchange.

SETTING THE TABLE

The AMF, which is responsible for overseeing the province's financial markets, found itself increasingly faced with situations of overlapping interests or the same targets as law enforcement. Reaching out to the SQ and RCMP, they voiced a need to encourage collaboration and communication among their three agencies.

The JSIU, born from that concept, is responsible for gathering intelligence to help further financial crime investigations in the province. Once all the intelligence is packaged, it then goes through the approval and consideration of the orientation committee and then the director's committee, which then assign the case to one of the three agencies for completion.

"We put on the table the names of the people who are subject to being investigated and we determine who's going to be investigating," says Philip Rousseau, the director of economic crime at the AMF and a member of the orientation committee. "If the RCMP is doing it, we can collaborate, we can help out, then we can step back and let it go."

Another aspect of the mandate is to detect and prevent fraud crimes in Quebec. By collaborating, not only does the unit prevent overlapping investigations into the same crimes or offenders, it's also able to proactively collect intelligence, develop human sources and generate leads — something regular investigators don't typically have the time for.

"We take pieces of information and we put the puzzle together and we get a clear picture of what's being done and who's doing what," says Cpl. Dominic Milotte, who has been leading the unit for the last two years. "And then, once investigators start on the case, they know where they're going and they don't waste time."

In 2012, the unit started 97 files. One third were opened intelligence files, while the remainder were the intelligence files actually shared between agencies. Rousseau likens the JSIU's work to setting the table so the investigators can dig in without having to worry about some of the potentially time-consuming prep work.

CLEARING THE CASES

Under the Memorandum of Understanding (MOU) that officially binds the team, all three organizations share the responsibility and authority equally. The MOU also allows them to share in other ways.

Because the province's two policing agencies have access to provincial and federal criminal intelligence databases, they're able to offer one another insight into information that may otherwise be inaccessible.

"Some of the cases we get, it's not clear-cut whether it's criminal or civil. It might not even be clear-cut for the police," says Rousseau. "The best thing this unit does is they get people talking to each other to get a better view of each case from a whole variety of sources."

Milotte adds that all the RCMP members have training and experience in criminal intelligence investigations. But that's not enough on its own to handle these kinds of investigations, which Captain Michel Hamelin, the officer in charge of the SQ's organized financial crimes investigation section, says can be very different from other types of crime.

"The biggest difference is often the sheer complexity of fraud schemes," says Hamelin. "We rely on the experience of financial crime intelligence officers to gather relevant information and, more importantly, understand how the crimes are being committed."

Each member of the unit brings something to the table that is unique to their experience, education and organization's focus. And that's the crux of why the files opened by the JSIU have been so successful so far, explains Milotte.

"We can't work in silos. It used to be like that a couple years back, everyone was protecting their intelligence but not sharing," says Milotte. "The value of putting all this together is that we're making stronger investigations, stronger intelligence probes, and in the end, because you get the whole picture, your investigations are more successful." ■

HOW CAN POLICE STAY AHEAD OF THE LATEST DIGITAL SCAMS?

THE PANELISTS

- **Det. Cst. John Schultz, intelligence analyst, Ontario Provincial Police, Canadian Anti-Fraud Centre**
- **Sgt. Marc Potvin, RCMP Financial Crime Unit, Fredericton, N.B.**
- **Cst. Kenneth M. Duff, Economic Crime Unit, Criminal Investigation Division, Royal Newfoundland Constabulary**

DET. CST JOHN SCHULTZ

In a world where spammers are pumping out more than 100 billion emails a day, Canadians are being victimized out of billions of dollars a year. The Canadian Anti-Fraud Centre receives more than 130,000 phone calls and 280,000 emails each year from consumers and businesses.

How can law enforcement agencies keep up with the advancements in communication technology and money transfers that criminals are using to their advantage? Organized crime is keeping up with this technology, so our challenge is to stay at par with them.

A mass marketing fraud scammer needs a method of communication and a means of collecting the money. Everything else is a fictitious story concocted to steal your money.

Communication

Communicating has never been quicker or easier: prepaid cellphones in fictitious names paid for with prepaid credit cards, Voice Over Internet Protocol (VOIP) calls, the use of free email addresses of the three major providers (Google, MSN and Yahoo) all situated in the United States, Skype situated in Luxembourg, Twilio — a virtual number in a cloud allowing calls back to your actual cellphone, Twitter, Tumblr, Hushmail and BlackBerry Messenger.

And then there's what's new: how about Google Glass being introduced in the fall of 2013, which will allow basic access to the Internet and text messaging, all through special lenses and mechanics built into the frames of a set of glasses.

Money

Bank-to-bank wire transfers, money sent in the mail, MoneyGram, Western Union, RIA, Green Dot, Ukash, email money transfers or bitcoin: money can be moved from country to country in a 24-hour period.

Whether it's the fraudster's message or their means of picking up or transferring the money, the scammer reaps the advantage of the time it takes police to investigate.

While traditional investigative paths are prudent and required, they must also catch up with the fraudsters. In today's world, criminals move money so fast from country to country that even a phone call can be too late to freeze transfers.

Using Interpol and Mutual Legal Assistance Treaties (MLATs) are essential to investigations and prosecutions, but to track the money and hit the fraudster where it hurts — by taking money out of the fraudster's pocketbook — requires some rethinking and adjusting of the rules.

Education and partnerships

Communicating with other law enforcement agencies is essential to provide timely, accurate intelligence to investigators, law enforcement leaders and the public.

The public must be informed of what is occurring in real-time. This proactive approach allows people to make educated choices so they don't become victims.

Law enforcement agencies, now more than ever, need the co-operation of private industry — the enablers of these new technologies.

The challenge is to build the partnerships necessary to identify the changes in technology, educate police and identify practical investigative methods to deal with it.

SGT. MARC POTVIN

North America is a market ripe with potential fraud victims. As citizens of a technologically developed country with one of the best economies in the world, Canadians are relentlessly targeted by digital scammers who strive to separate them from their hard earned money, or even worse, from their own identity.

Phishing, Spear Phishing, Vishing, SmiShing, 419 scams, Scareware scams, there's even a "Scam Victim Compensation Center Scam" that targets those who've already been victimized. Digital scams are so varied that an entire jargon is slowly making its way into our culture.

For police to keep up with this new frontier of fraud, they will have to adjust the way they prevent and enforce these types of crimes.

Fraud will never be eradicated through enforcement alone, and prevention efforts to reduce the number of potential victims will need to form a significant portion of the strategic planning.

Fraud-prevention campaigns must focus on fostering healthy skepticism in Canadians, to the point where most will be able to complete the saying, "If it's too good to be true..." (it likely is).

Unfortunately, when facing financial hardship, scams become believable to victims looking for a quick way out, especially if they're delivered in a new and innovative way. This is why scammers do the most damage to citizens who can least afford it, and why police agencies need to constantly innovate their prevention strategies.

While seniors remain the most vulnerable, prevention efforts need to reach all Canadians. For example, just in time for the arrival of Web 2.0, some agencies are reaching a larger audience and relying less on traditional media by experimenting with the use of social media to enhance prevention campaigns.

These efforts target 20- to 40-year-olds, who are technologically savvy, but still falling victim to digital scams in large numbers. Additionally, police agencies should consider including senior high school students in fraud prevention campaigns so that young adults become aware of digital scams as they enter the workforce.

Still, once someone has been victimized, a relentless pursuit of justice is expected

from police. Through the passing of the 2011 *Standing up for Victims of White Collar Crime Act*, Parliament gave Canadian police agencies unprecedented tools to fight fraud in all its incarnations.

Despite having these tools, it's been my personal experience that investigations often stall when it's discovered the suspects operate a continent away.

In practical terms, police agencies have a playing field that is defined by their jurisdiction, while digital scammers have the entire world as their playing field. With information technology developing rapidly, an international systemic effort similar to the Financial Action Task Force on Money Laundering may be required.

Such a commitment from the international community would enable agencies to collect and share information on digital scams and the crime groups involved in them, enable some type of regulation of electronic money transfer services, and support effective and timely enforcement against this trans-border crime.

On a local level, both law enforcement and prosecution teams need to ensure they attract, develop and retain specialized staff who can effectively prevent, investigate and prosecute technological fraud.

Agencies that value operational flexibility at the expense of financial crime specialization will fall behind in the fight, and will do so at the peril of the thousands of digital scam victims each year.

CST. KENNETH M. DUFF

This is a complex problem with no quick solution. A number of things can be done to minimize the success of fraudsters and make these crimes less attractive to criminals.

Through the media and public speaking opportunities, police departments must educate the public about the many scams circulating on the Internet. An informed Internet user can quickly identify and avoid becoming a victim of these scams.

Specialized police units tasked with investigating digital crimes are typically focused on bigger scams or more serious crimes such as online child exploitation. This often leaves a gap where the crimes in which dollar amounts don't meet the threshold to be investigated by cyber investigators in specialized units are assigned to patrol officers or investigators in other units.

These officers, through no fault of their own, haven't been trained in how to conduct these type of investigations. All police officers need training and mentoring programs that will help them develop the skills to successfully complete these types of investigations. This training should be part of basic training in the same way other investigative techniques are.

In recent years, providers of web-based email addresses have eliminated the senders IP address from email headers and replaced them with their own IP address. In order for police to track the origin of emails sent for criminal reasons, police must now seek judicial authorization to get the senders IP address.

Once police get this information, they need a further authorization to be served on the Internet service provider (ISP) asking them to identify who was using the IP address. Two steps where there should be, and used to be, one.

Because the providers of many of these web-based email addresses are located outside Canada, an MLAT is required. There is very little appetite on the part of most to assist police in obtaining an MLAT for a crime of this nature.

An IP address in an email header gives no personal information. It just shows the ISP of the sender of the email, but helps the ISP identify the sender of the email and police quickly see where the fraudsters are operating from. Legislation is needed to prohibit corporations and the providers of web-based email addresses from blocking or removing the sender's IP address.

More authority should be given to the courts so they can give sentences that make these crimes less attractive to the culprits. Canada Border Services Agency also needs more power to swiftly remove non-residents convicted of these crimes, especially those who appear to have no other purpose for being in Canada.

These types of crimes are seen as non-violent and therefore not serious in nature. However, the damage done to a victim's personal credit can be exhausting to repair. ■

NFIB

According to Detective Chief Inspector Oliver Little of the NFIB, the U.K.'s national reporting system is preventing and disrupting more fraud, and saving the public and police agencies money.

ACTION FRAUD

THE U.K.'S ACCESSIBLE, VICTIM-FOCUSED SERVICE

By Detective Chief Inspector Oliver Little, deputy director, National Fraud Intelligence Bureau, United Kingdom

The United Kingdom (U.K.) identified in 2006 that the country as a whole, from private citizens and the public sector, to small companies, major high street brands and corporations, was suffering from a rising tide of fraud.

Fraud was causing more loss and becoming more complex with the channel shift to the online forum. Fraud was funding terrorism. It was also a new lucrative safer haven for organized criminals who were drawn to fraud because it could be done at arm's length, it was low risk because police weren't encouraged to prioritize it, and the sanctions against fraud, when compared to an armed robbery or drug running, were very low.

Both capability and capacity were stretched by the circumstances of the times.

NEW APPROACH NEEDED

The start point in turning the tide was a strategic review conducted by the Attorney General's Office. It painted a stark picture of the threat and found that the law enforcement response was lacking focus, strategic vision and co-ordination.

Among the many recommendations was a clear case for a single reporting mechanism and a single repository for fraud intelligence. Within the U.K. alone, there were 43 separate police forces taking victim reports with wide variations in the standard of advice and care.

The information obtained from victims was then kept within the crime and intelligence systems of those 43 forces, effectively in silos. Victims suffered and fraudsters were able to reap the benefits of the system failings in running simple, preventable, cross-border scams, and digging their hands deeper into everyone's pockets.

A huge amount of hard work has gone into realizing the key objectives of the review, and the United Kingdom today is a more hostile environment for fraudsters as a result.

ONE-STOP SHOP

In 2010, the U.K. created a single national reporting mechanism.

Action Fraud offers a simple, accessible, victim-focused service. It gives individual and business victims one place to report their crime, either by telephone or online, and gives them access to the services they need to recover from their loss and protect themselves from falling victim again.

Not all of the contact they receive amounts to crime. Last May, Action Fraud received 63,690 contacts from the public, 31 per cent of which were identified as crimes. This centralization delivers a significant cost saving to every force in the country in the

handling and triage of fraud calls.

While the trained advisors within Action Fraud listen to the victims, they convert their story into the structured data needed to make the single repository — the National Fraud Intelligence Bureau (NFIB) — do its job in preventing, disrupting and enforcing these crimes.

The NFIB is the United Kingdom's front line in combating fraud. Hosted by the City of London Police, which has a long and distinguished history in fighting fraud, it's comprised of specialist intelligence, crime and disruption teams that address fraud in a holistic way. The bureau delivers an appropriate response from across enforcement, including disruption, prevention and education.

"KNOWFRAUD" DATABASE

The NFIB received 19,722 crimes from Action Fraud in May, and these were added to the NFIB's KnowFraud database where they are combined with regular feeds of confirmed fraud intelligence from a range of public and private sector partners.

The custom software links all reports with matching entities and creates networks. By entities, we mean those facets of the crime that link the fraudster to the crimes and may provide an evidential trace. Practically speaking, this includes the suspect's name, vehicle, phone numbers, web addresses, email addresses, bank accounts and so on.

Linked networks of crimes are scored based on predefined, but flexible, rules that objectively assess viability. Those networks identified as viable are then reviewed by the NFIB's crime team to identify what, if any, further research is required to peel back more layers of the deception and identify the person or group responsible.

The network is then allocated to the most appropriate police force or law enforcement body to take enforcement action. Police forces will investigate the crime networks and update the system on the results, which will include the suspects' identities, enhancing the database further.

The system is designed to identify commonality, thus allowing police to find the most prolific and harmful fraudsters and methods.

The disruptions team uses the same fraud data to pick out those key enablers to fraud — telephone numbers, bank accounts, websites and email accounts — causing the most harm. They engage with service providers to shut down services.

Due to the cross-border nature of fraud, between 25 and 33 per cent of all crime reported by U.K. victims is caused by criminal activity overseas. Two prominent examples and focus areas of the NFIB are cyber and telephone deceptions that originate in India. The NFIB works with overseas law enforcement to combat this type of fraud.

The intelligence team is comprised of analysts and researchers who provide access to the database with the counter-fraud community. They also analyze all of the available information, drawing together counter-fraud partners to produce tactical support products on organized crime groups as well as trends and alert products.

MAKING THE LINK

A simple crime case study is ticketindex.net. This website was established promising tickets for Take That concerts, which the fraudster never held or could supply. Victims, who were spread across the country, each suffered a loss of £40 (C$64).

Prior to this system being in place, the victims would have struggled to report these low-value crimes to a local police force. A local force with a handful of victims in its jurisdiction wouldn't be obliged to investigate without evidence of a location for the offence.

When these crimes occurred in the United Kingdom, the staff in Action Fraud started to identify an increase in calls about the same scam within hours and notified NFIB. The crimes were all linked by the same web address.

Very quickly, the scale of the harm was clear — hundreds of victims were affected. The case was prioritized and the NFIB crime team produced a comprehensive investigation package, while suspending the website and payment enabler services.

Although the research identified a suspect in London, the scale and scope of the offences met the criteria for the City of London Police who, as a national lead force for fraud, had the capability to arrest the suspect and prosecute.

From its overview of reported crime, the NFIB can put the threat from each crime type into strategic context. For example, boiler room or share sale frauds don't account for a large proportion of the victims who report frauds. But they do constitute the biggest losses over the last financial year with an average loss of £54,000 (C$86,000) per fraud. This is an international problem and an organized crime problem, with multiple groups targeting vulnerable victims in the U.K. and overseas.

Not every fraud can be investigated as the number of groups involved outstrips the enforcement capacity. The ability of our system to quickly link multiple criminal brands by their recipient bank accounts or the source IP address of the website, allows us to identify the groups causing the most harm. We then refer those groups to the City of London Police fraud squads for enforcement and provide ongoing investigation support.

Our proactive interventions team circulate the recipient bank accounts for investment fraud to the banks. When banks receive an alert from NFIB, they can choose to exit their relationship with the customer and close the account. Any money recently arrived from a similar transaction can be returned and any money on its way is sent back to the victim.

Over the past financial year, the NFIB has produced 389 investment fraud bank alerts with an estimated saving of £3.4 million (C$5.4 million).

Outside of the enforcement or disruption outcomes, there are still a huge range of options and benefits from the effective use of this single repository.

We can identify seasonal trends such as online shopping around Christmas and dating fraud in February. We can produce creative tailored alerts with industry partners to prevent fraud and then use the database to show what impact we've had on the problem.

The NFIB is both a tactical and strategic tool for managing a complex problem. It can visualize the whole scope of reported fraud in the United Kingdom, showing police where the threat and risk is. It can also point to how and sometimes where to catch someone causing harm right now.

The creation of the NFIB coincided with austerity measures biting into all public services in the United Kingdom. Our ability to organize large amounts of data and seemingly disparate strands into an ordered structure, showing what's important and what's achievable, could not have arrived at a better time. ■

Toronto Police Service

Messages about fraud prevention reached 2.3 million people at a fraud awareness event held in Toronto last February.

LET'S TALK FRAUD

RAISING AWARENESS ONE TWEET AT A TIME

By Detective Sergeant Cameron Field, Financial Crimes Unit, Toronto Police Service and Kristen Rose, senior communications officer, Financial Services Commission of Ontario

Financial crime isn't a popular topic in the media or at the dinner table. But it is something that victimizes a growing number of Canadians each year, many of whom are too embarrassed or ashamed to tell anyone what happened.

Even though it's estimated that fraud costs Canadians more than $10 billion each year, the RCMP reports that an overwhelming nine in 10 Canadians who are victimized don't speak to anyone about it.

Every day, the Financial Services Commission of Ontario (FSCO) and the Toronto Police Service (TPS) Financial Crimes Unit deal with people who have been victimized by fraud and other schemes, and each was finding it difficult to raise awareness about fraud prevention.

Fraud prevention tends to be a hard sell for mainstream media who gravitate towards stories involving multiple victims and large dollar losses — not tips on ways to protect against fraud.

OUTREACH ON FINANCIAL CRIME

Both FSCO and TPS began using social media to reach out directly to the public and speak to people about fraud prevention. Platforms such as Facebook and Twitter allow for information to be sent out with the opportunity of having the message shared by hundreds if not thousands of people. In certain cases, the reach is in the millions.

Social media is also extremely cost-effective and simply requires the time commitment of a few dedicated employees. At a time when many public agencies face considerable pressure from shrinking budgets and workforces, social media offers a huge bang for the buck.

In the fall of 2012, FSCO and TPS decided to compare notes on the time that each organization spends using social media to raise awareness about fraud prevention. It became obvious that by working together, they could reach significantly more people.

There were two opportunities that would greatly assist both organizations as well as dozens of others that play a role in public outreach on financial crime:

- Establish a group dedicated to increasing consumer awareness about fraud, scams and other forms of financial crime through social media and other digital platforms
- Create an interactive forum where the public could learn about protecting themselves from fraud, scams and other forms of financial crime and have access to subject matter experts

SOCIAL MEDIA WORKING GROUP

In November 2012, FSCO and TPS established a Social Media Working Group, an informal group committed to enhancing public outreach on fraud, scams and other forms of financial crime through social media and digital platforms. The group envisioned the following benefits:

- Exponentially amplifying messaging through social media platforms
- Opening up lines of communication between agencies
- Providing opportunities to learn from one another's digital experiences

- Serving as a forum for sharing best practices

One of the unique aspects of this group is that it meets quite frequently. Every two to three months, the majority of members meet to discuss upcoming events, trends in social media, successes and failures and future campaigns requiring the larger group's attention.

Although the group is based in the Greater Toronto Area, its membership is expanding to other areas of Canada. The group is comprised of communications professionals, investigators, police officers and other professionals.

The unique composition of the group lends itself to the great reach experienced on social media:

- Financial Services Commission of Ontario
- Toronto Police Service
- Bank of Canada
- Crime Prevention Association of Toronto
- Canadian Anti-Fraud Centre
- Insurance Brokers Association of Ontario
- Ontario Ministry of Consumer Services
- Ontario Provincial Police
- Royal Canadian Mounted Police
- RBC Bank
- Real Estate Council of Ontario
- Insurance Bureau of Canada
- Canadian Association of Accredited Mortgage Professionals
- Canadian Healthcare Anti-Fraud Association
- Investor Education Fund/Ontario Securities Commission
- Scotiabank
- Canadian Bankers Association
- Financial Consumer Agency of Canada
- First Canadian Title
- Canadian Life and Health Insurance Association
- TD Bank
- The General Insurance OmbudService

The group's first joint effort took place on Feb. 28, 2013, when it kicked off Fraud Prevention Month with an event in Toronto.

The launch was attended by a large number of media outlets due, in part, to the persistent engagement of the group with their media partners along with social media outreach. Two seniors who had been victimized by fraud attended the event and shared their stories.

The event also featured a panel of senior representatives from participating organizations, the unveiling of a digital fraud prevention campaign produced by Toronto college students and information displays from group members' organizations.

During the entire month of March, group members continually cross-promoted their campaigns, supported social media messaging of other members and, in some cases, launched joint campaigns or public service messaging. The united voice of the group caught the attention of the mainstream media and resulted in millions of people sharing fraud prevention information online.

According to statistics gathered by FSCO, messages about fraud prevention reached, on average, close to 1.7 million people each week of Fraud Prevention Month through Twitter alone. The peak, at the launch event, reached 2.3 million people through this single platform.

FRAUD CHAT ON TWITTER

To get more people talking about fraud online, FSCO and TPS launched #fraudchat — a weekly Twitter chat on topics related to financial crime and fraud prevention.

The fraud chat forum takes place each Thursday night from 9 p.m. to 10 p.m. Eastern Time and is co-moderated by the co-authors of this article, Detective Sergeant Cameron Field of the TPS Financial Crimes Unit and Kristen Rose, a senior communications officer at FSCO. To follow the chat, people simply need to open a Twitter account and follow the fraud chat hashtag on Thursday nights.

This campaign gives people regular access to a police officer and a representative from a financial services regulator to ask questions about fraud prevention.

In addition, fraud chat frequently features subject matter experts on different types of frauds and scams. For example, it has featured representatives from the Insurance Bureau of Canada in chats on auto insurance fraud and staged motor vehicle collisions. Similarly, a recent fraud chat on identity theft featured representatives from the RCMP and Canadian Anti-Fraud Centre.

To ensure fraud chat was increasing online conversation about fraud, scams and other forms of financial crime, FSCO recently compiled statistics on its reach. The results made it clear that the chat was a success, and that there was a growing appetite for fraud prevention information online:

- Fraud chat reaches, on average, 746,924 people each week with fraud prevention messages
- Since the launch of fraud chat, conversation on romance scams on Twitter has increased by 245 per cent
- Conversation on insurance fraud on Twitter has increased by 90 per cent
- Conversation on home improvement scams on Twitter has increased by 65 per cent
- Conversation on seniors and fraud on Twitter has increased by 40 per cent.

What was evident in these statistics is that there is a real willingness for Canadians to talk about fraud and scams on social media. Anecdotally, many followers expressed gratitude to be given a forum to discuss being scammed or defrauded. Given the right setting, Canadians are more than willing to talk about their experiences with financial crime and scams.

FSCO and TPS are now planning the future of fraud chat for the months and years to come. There is great potential in expanding the program so that victims of scams and fraud can not only seek guidance from experts and industry professionals but also help other victims through forums and other social media activities. The group is considering supplementing its weekly Twitter chats with regular webcasts to increase the quality of the conversations with the public and make them even more interactive.

When Canadians get defrauded or scammed, there's a level of embarrassment and shame that prevents them from reporting it to authorities and to their families. Through the Social Media Working Group and fraud chat, those barriers are taken down through enhanced public education and meaningful dialogue with experts and fellow victims.

The ultimate goal is to prepare Canadians to spot scams and frauds before they fall for them. The benefits of reducing victimization affect every area of Canadian society. This seems to be a good start. ■

CROSS-BORDER FRAUD

By Cpl. Satish Tarachandra, Toronto West Financial Crime Section, RCMP

In August 2009, the RCMP Toronto West Financial Crime Section's Payment Card Team was contacted by corporate security investigators at a Canadian bank and told that a group of suspects was committing large-scale identity theft, mail hijacking, impersonation of bank clients and account takeover frauds.

The suspects were going into various branches across Canada with forged client identification, accessing victims' accounts and withdrawing funds. Investigators soon learned that multiple financial institutions were targeted by the organization.

During the investigation, police identified Nigerian citizen Ife Eguakun as the directing mind and active participant in 34 separate frauds across Ontario, Alberta and British Columbia between March 2007 and September 2009. The losses from these frauds exceeded $1 million.

METHODOLOGY

The frauds typically began with Eguakun identifying victims through various means, including credit bureau checks.

Eguakun would then call the bank and ask that the client's mail be re-directed to another mailing address, changing the client's address in the bank's system.

He would make another call requesting a replacement debit card. Based on this call, the bank would mail out a replacement card to a mailbox that Eguakun could access. A week or two later, Eguakun would again call the bank to change the client's address back to the original to avoid detection.

Some time later, Eguakun or one of his accomplices would go into a bank with a fraudulent client card and false identification in the name of the bank's client. He would tell the bank staff that he had forgotten the personal identification number (PIN). The bank staff would then request identification and, upon being provided a realistic-looking ID card, would help Eguakun or his accomplice change the PIN.

Eguakun or his accomplice would then withdraw or transfer money from the account. To avoid suspicion, he would transfer small amounts at first, then larger sums later on.

When these frauds were identified through surveillance in August 2009, the corporate security section at the bank sent out an alert to all its branches requesting they be notified if something of this nature occurred.

Eguakun was identified in 11 of these frauds. His accomplices were captured on surveillance conducting the remainder of the account takeovers.

CAUGHT IN THE ACT

On Sept. 25, 2009, the team set up surveillance at an immigration sign-in location in Ontario, where Eguakun was scheduled to present himself that morning. Investigators learned that Eguakun's family members had advised immigration officers that Eguakun was sick in bed at their residence.

During this time, the bank called police to inform them that Eguakun and an unidentified man had been seen committing bank frauds in Alberta.

Eguakun and an accomplice were arrested the same day on an aircraft after it arrived in Toronto. In his suitcase, police found $11,280, several counterfeit Ontario and Alberta driver's licences, social insurance cards, credit bureau print outs and sheets of paper containing detailed handwritten RBC (Royal Bank of Canada) bank client profiles.

North Bay Police had also searched a hotel room where Eguakun had been staying while committing frauds in North Bay. They found additional false documents and incriminating evidence.

Two of Eguakun's accomplices provided taped statements to police that Eguakun was the directing mind behind the criminal organization. He taught them how to commit the frauds and provided them with the phony documents and client information they required. They would give all the money to Eguakun and he would give them a small percentage for their role.

While Eguakun was on bail for these offences, he attempted to commit another fraud in Brampton, Ont. The bank teller became suspicious and Eguakun fled, leaving his false ID cards behind.

Eguakun wasn't aware that he'd been identified attempting to commit this fraud while on bail and, as per his bail conditions, signed in to the Toronto West RCMP detachment in Milton, Ont. He was arrested shortly thereafter following a brief foot chase with police.

CONCLUSION

Six members of this criminal organization were convicted in Brampton Provincial Court of account takeover and identity theft-related bank frauds committed throughout Canada.

Eguakun and two other members of the group pleaded guilty under Section 467.12 of the *Criminal Code* for the commission of an offence for the benefit of a criminal organization.

Eguakun pleaded guilty for instructing another person to commit an offence for the benefit of a criminal organization. These criminal organization-related offences are very rarely obtained in any criminal investigation, particularly in the financial crime context.

The successful disruption of this criminal organization was mainly due to the use of traditional investigative techniques by a small investigative unit in conjunction with real-time information and partnership provided by corporate investigators of the financial services industry. ■

Ife Eguakun is captured on surveillance supervising another member of his group to commit a fraudulent bank transaction.

RCMP

DIRTY BANKS EXPOSED

FORMER AGENT AIRS DETAILS OF CAREER-MAKING CASE

Robert Mazur was a college student studying business when he saw a posting for a co-op position within the Intelligence Division of the Internal Revenue Service (IRS). Not knowing entirely what that entailed, Mazur applied for a summer job that resulted in a career working undercover investigating drug cartels and corrupt world leaders. Gazette *writer Sigrid Forberg spoke with him about his recent memoir,* The Infiltrator*, on his work fighting financial crime.*

Courtesy of Robert Mazur

Robert Mazur (right) poses with a pilot in front of one of the jets he used in his undercover operation investigating the financial crimes of high-level drug traffickers.

YOU STARTED YOUR JOB AS A SUMMER STUDENT. WHAT MADE YOU STAY?

The option of being an investigator of financial crimes versus being a Chartered Professional Accountant (CPA) and counting widgets, to me, was pretty exciting. I was in a section of the IRS that really focused more on using criminal tax offences to prosecute drug traffickers, corrupt politicians and organized crime figures. Really, it was the "follow the money" section that went after people who certainly seemed well worth going after.

One of the first cases I saw being worked on was Frank Lucas. That was a case of one of the biggest heroin traffickers in the United States at the time who was importing large quantities of heroin into the U.S. in body bags of soldiers being brought back from Vietnam. We were surveilling their couriers who were bringing duffel bags full of cash to the bank. And so the evidence we gathered was used not just to go after the criminal organization, but to go after the bank for not complying with the *Bank Secrecy Act* and intentionally failing to file the forms that would have otherwise been required for cash deposits over $10,000.

WHAT DOES IT TAKE TO BE A GOOD INVESTIGATOR IN THESE CASES?

I've met so many investigators that have extraordinary talents but they're all in different areas. I think one of the things that's most important is to recognize what your strong suit is and to exploit it. But then also, at the same time, to work on developing those things that you are maybe not that strong in because you really need to be able to answer any challenge that you might be faced with. I think managing informants is probably one of the highest risk tasks that officers have. I know, at least in my view, the mismanagement of informants has led to the demise of careers. Another one of course is actually having an ability to communicate and to communicate effectively. That is going to have an impact on your ability to manage, your interviewing techniques, your performance and your ability to, unfortunately, as we sometimes need to do, sell your case and get resources from management.

WHY DID YOU WANT TO WRITE A BOOK?

Well, the core reason was that I think it tells a very unique story and is an opportunity for the public to see something that I have referred to for three decades now as the elephant in the room. How is it that we can have $400 billion a year generated from the sale of illegal drugs, and seize only — at least with respect to U.S. authorities — less than $1 billion a year? That's one fourth of one per cent. Clearly, there are very sophisticated professionals within the international banking and business community who routinely market this money and the laundering of this money. And to be able to expose a real story about the involvement of the board of directors of the seventh largest publicly held bank in the world helps people to understand what the economics of crime is really all about.

WHAT DO YOU HOPE LAW ENFORCEMENT WILL TAKE AWAY FROM THE BOOK?

A willingness to think outside the box. When you look at the facts of that whole operation, it certainly is outside of the cookie cutter ideas on how to approach a long-term undercover money laundering operation.

As long as it's done in a professional manner and in a professional setting, it's important for officers to share their different perspectives and their concerns. That is something that I think we consistently did in our operation and I think it translated into success because we did a lot of things that hadn't been done before. Unless you really make the effort to try to get agencies to do things a bit differently, we're going to end up with techniques that are so common and so easily detectable that our success rate is going to diminish tremendously. ■

CO-OPERATION BEYOND THE TYPICAL

TASK FORCE UNCOVERS MASSIVE IDENTITY THEFT RING

By Supt. Wade Setter, Minnesota Bureau of Criminal Apprehension

In August 2012, Julian Okeayaninneh, 44, of California, and Olugbenga Temidago Adeniran, 36, of New York, were each sentenced to more than two decades in federal prison for their roles in one of the largest known cases of identity theft in U.S. history. And now, the investigation that uncovered the crime is changing the way law enforcement agencies view collaboration among local, state and federal agencies.

The investigation started in 2009 when two members of the Minnesota Bureau of Criminal Apprehension's Financial Crimes Task Force compared notes on two identity theft cases they were working separately. Similarities between the two cases led the task force to launch an investigation into whether these two cases were components of a larger, organized criminal enterprise.

What they and other task force members eventually found was a sophisticated system of identity theft, bank fraud, counterfeit cheque manufacturing, credit card fraud and money laundering involving more than 200 participants in 11 states, and more than 8,700 victims across the globe.

The fraud was carried out by a broad, deep, multi-tiered network of criminals.

Organizers recruited bank insiders to provide banking and customer identification information to other conspirators who produced massive amounts of counterfeit identification materials including licences, credit cards and access cards. These materials were then used by additional conspirators to draw from existing accounts or open fraudulent accounts.

They created additional documents — fake passports, driver's licences, hundreds of credit cards bearing different names, blank cheque stock and more — and used them to commit further crimes. Monetary proceeds from the illegal activities were laundered through financial institutions via bulk cash shipments.

The first arrests in the case, in 2009, included lower level players and bank employees, many of whom pleaded guilty or reached proffer agreements to provide information about the conspiracy, its structure and its reach. Then, in the fall of 2010, the arrest of a foot soldier led to information about a certain California storage locker that proved to be the most significant break in the case.

Task force investigators located and searched the storage locker in December 2010 and found thousands of stolen identity documents, including the following:

- 8,700 victims' identities, IDs and bank account information
- $18 million face value of commercial cheques
- 140 passport photos
- 30 IDs with kingpin's photo
- 90 drivers licences in the names of others
- Credit card reader and re-encoder
- 500 credit cards in the names of others

This discovery revealed for the first time the full scope of the victimization. Previously, investigators knew there were many suspects in a well-organized operation, but didn't know just how many victims existed.

As investigators carried out their raid on the locker, they caught another break. The kingpin of the network, Julian Okeayaninneh, showed up at the facility and, unaware that investigators were there, went to his locker.

He provided a false name and denied the locker was his, but investigators matched security camera images taken when he arrived that day to the photo on the storage locker rental paperwork he filled out in March 2006. Evidence obtained during the raid revealed that the scheme had been playing out since that time. Okeayaninneh was taken into custody.

GAINING CO-OPERATION

In 2011, the U.S. Attorney's Office, the U.S. Inspector General, the U.S. Department of the Treasury's Office of Comptroller of the Currency and the Federal Deposit Insurance Corporation were brought in to convince large financial institutions of the value of their co-operation.

The financial institutions, understandably concerned about erosion of public trust in their institutions, were initially reluctant to co-operate, and those discussions stretched more than a year.

In the end, all employee-suspects were allowed to continue working until they could be caught in the act — and in most cases beyond that time, until the full extent of the scheme was revealed. Investigators also developed confidential informants within the banks who pointed investigators to specific employees.

"Developing these informants was particularly challenging because investigators at this point did not know which employees in those institutions were committing the crimes," said Minnesota Financial Crimes Task Force Commander Patrick Henry.

One reason investigators needed the financial institutions' co-operation was so that, after suspects in the banks were identified, investigators could set up accounts that would allow them to collect evidence by following audit trails. This prospect was not only expensive, but extraordinarily delicate, as it required banks to knowingly allow fraud to continue.

In addition, bank investigators provided outside investigators access to information that would ordinarily be difficult to obtain with a subpoena. While the process was successful, it wasn't easy. Investigators needed to be cognizant that banks couldn't operate as agents of law enforcement, and investigators could not disclose investigative data to the banks.

Task force investigators had to develop a way to securely deliver private data (names of 8,700 victims) to bank investigators to establish whether the banks held real or fraudulent accounts. This required creating a technology solution that would merge data from the many disparate record-management systems belonging to investigators, banks and credit card companies. The data was also adapted to be checked against the Federal Trade

Commission's list of identity theft victims.

IDENTIFYING THE VICTIMS

Investigators worked with financial institutions, the U.S. Federal Trade Commission and other law enforcement agencies to identify where real and fraudulent accounts existed under known victims' names.

They also worked to identify persons who hadn't realized they'd been victimized or hadn't reported it. In those cases, investigators tracked down victims individually. This required co-ordination among local, state and federal agencies, and agencies in states and jurisdictions where both the crimes were committed and where victims were identified (for purposes of obtaining reports).

Investigators also worked with local agencies and other contacts nationwide to subpoena witnesses and victims to appear in court and testify in Minnesota.

DEVELOPING THE TOOLS

Managing an investigation with so many people, so many locations and so many targets proved extraordinarily challenging. Investigators created a tiered chart of suspects (more than 200) that focused the investigation and helped with allocation of resources. It also provided a road map as the complex structure of this criminal organization was revealed.

Investigators also invented a system for tracking more than 300 pieces of evidence that had to be sortable by individual victim, by suspect and group of suspects, and by associated bank or banks.

In addition, investigators developed ways to share criminal justice data between multiple local, state and federal criminal justice agencies, every one of which provided a unique set of data-compatibility issues.

Investigators shared case information with law enforcement agencies, financial institutions and merchants through the Minnesota Crime Alert Network. Investigators used the state's fusion center — the Minnesota Joint Analysis Center — to gather information from state and federal authorities about other ongoing investigations and intelligence relevant to this case. These tools and this targeted-audience approach are unique to Minnesota.

Minnesota Financial Crimes Task Force

A security camera captured this image of Julian Okeayaninneh as he arrived at the storage facility the day he was taken into custody.

BRINGING THE OPERATION TO LIGHT

From the beginning, investigators mined massive amounts of social media and other open-source data to gain information about their suspects and planned or executed criminal activity. The criminals had posted still and video images of themselves and co-conspirators with money and other items obtained via this enterprise.

Investigators also gained information about criminal associates who participated via social networking connections and posts. They worked quickly to identify suspects, shore up their cases and increase their chances of successful prosecution.

"We knew suspects had real and false passports, significant financial support and network connections all over the world — in other words, fleeing would be relatively easy," Henry said.

In March 2011, 12 defendants including the network kingpin, some of his top managers and bank insiders were indicted on a total of 126 counts that included bank fraud conspiracy, bank fraud, aggravated identity theft, money laundering and more.

Nearly two dozen others arrested in 2011 and early 2012 pleaded guilty to various charges. All but two suspects brought to trial were convicted in February 2012.

The leader of the organization, Julian Okeayaninneh, was sentenced to 28 years in federal prison — the longest sentence ever imposed for this type of crime.

This investigation required collaboration with non-criminal justice partners as well as criminal justice partners at the local, state and federal levels. Investigators utilized information from proffers and informants, investigative tools from private business and criminal justice agencies at all levels, and intelligence drawn from multiple criminal justice sources.

Investigators relied on expertise and technology at every level of law enforcement. They developed multiple systems to share data with disparate records management systems and developed a tiered system to track information on more than 200 suspects.

To date, their efforts have resulted in 31 ring members convicted or pleading guilty in this $100 million-dollar scheme.

Phase two of the investigation is ongoing. ■

The Minnesota Financial Crimes Task Force investigates financial crimes related to identity theft, with a special emphasis on organized criminal enterprises. The task force is comprised of multi-jurisdictional law enforcement agencies working together to provide investigative expertise and resources.

TRUST ME, I'M JUST LIKE YOU

THE PREDATORY PRACTICE OF AFFINITY FRAUD

By Frank S. Perri, JD, CPA, CFE

Affinity generally refers to a sense of kinship based on characteristics common to a specific group. Investment scams that prey upon members of identifiable groups, such as racial, religious and ethnic communities, the elderly, professional groups, or other types of identifiable groups, are called affinity fraud. The offenders who promote affinity scams frequently are — or pretend to be — members of the group.

Attacking affinity fraud is inherently difficult because group trust is often so powerful that many fall prey to such scams.

New immigrant groups are susceptible to affinity fraud because they're often isolated from the larger community and are unfamiliar with the local laws and customs regarding investments.

In the United States, affinity fraud has been conservatively estimated at $50 billion a year (*Economist*, 2012). Recently, over the past several years, citizens of Utah alone who belong to faith-based organizations have been defrauded through the practice of affinity fraud of more than $1.5 billion dollars (Morgan, 2011).

EASY CREDIBILITY

Often, the fact that a person or organization shares similar characteristics to his or her target audience is enough to make them appear more credible.

The predatory practice of affinity fraud is widely observed in religious circles. Defrauding investors in church-based settings is particularly effective because con artists can tout fraudulent investments to an entire congregation. However, perpetrators also use Internet sites, ethnically affiliated media, conferences or other social gatherings to gain access to members of a specific group.

These offenders typically enlist respected religious leaders from within the group to spread the word about the scheme by convincing them that a fraudulent investment is legitimate and worthy of advancing the social and economic interests of the group. Once convinced, the leader becomes the offender's pawn, convincing his followers that the offender is trustworthy.

Affinity fraud undercuts the usual warnings about investment schemes so that the normal process of cautious skepticism is replaced by social banter. These fraudulent investments often come to the victim's attention through contact from a friend, colleague or someone who inspires a bond of trust.

Perpetrators of such scams also design their investment opportunities to appeal to specific groups. For example, literature or other presentations stress their shared heritage, language or identity with other group members. With these techniques, perpetrators use group affinity as a means of legitimizing themselves and their fraudulent investment programs.

Attacking affinity fraud is inherently

REDUCING THE INCIDENCE OF AFFINITY FRAUD

Experts recommend the following to avoid affinity fraud and other scams:

- Avoid investing if the promoters say they don't have the time to put the particulars of the investment into writing or that they're unregulated because they're for religious institutions.
- Be wary of investments that are pitched as once-in-a-lifetime opportunities, particularly when the promoter bases the recommendation on "inside" or confidential information.
- Be wary of investments that promise spectacular profits or guaranteed returns with little or no risk.
- Obtain, in writing, details about the risk of the investment, financial statements, any conflicts of interest and procedures to get your money out.
- Ask for neutral professional advice from an outside expert not associated with the salesperson to evaluate the investment.

—Perri & Brody, 2013

difficult because once trust is established, not only are investors less likely to fully investigate the "opportunity," but they're also less likely to believe they have been defrauded. Even when they realize it, they're less likely to report the fraud outside of the group.

Church-based affinity fraud poses special problems for securities regulators because victims are reluctant to inform investigators that they've been scammed. At times, the reluctance to involve securities regulators can be attributed to a negative impression of law enforcement and a desire to resolve the problem within the group rather than outside it.

PERSUASION AND INFLUENCE

When a person seeks to persuade another to do something, social psychology has identified several ways to achieve this.

A direct, central route to persuasion relies on presenting a logical argument, which prompts the listener or reader to think deeply about an issue. However, applying logical thinking may not necessarily succeed as a strategy of persuasion because there may be facts that reveal the illegitimate or fraudulent activity.

An indirect route to persuasion relies on decision-making shortcuts that serve as distractions causing the victim to bypass logical thinking and accept what's being said with very little thought.

Consider the sales material that convicted fraud offender Vaughn Reeves used to train church members to sell securities to other church members. The material stated, "Never sell the facts, sell the warm stewardship of the Lord" (AP, 2010).

Several other factors can result in effective persuasions: authority, social proof, similarity and reciprocation (Luo et al., 2011).

For example, people are conditioned to respond to authority figures without diligently verifying their legitimacy. In affinity fraud schemes, the offender will often target the leader of a group — an authority figure who others will unquestioningly follow.

When making a decision, another mental shortcut is to see what other people in the group are doing or saying, then follow suit. This phenomenon, known as social proof, can prompt someone to take actions that may be against their own self-interest without taking the time to consider them more deeply. Social proof is evident in affinity fraud.

Identifying someone as having characteristics that are identical or similar to one's own provides a strong incentive to adopt a mental shortcut in dealing with that person. This is illustrated by Ronald Cass, Dean Emeritus of the Boston University School of Law, who commented on Bernard Madoff, who was convicted in 2009 of securities fraud: "You had every reason to trust the guy. He looked like and sounded like you and your friends."

Finally, a well-recognized rule of social interaction requires that if someone gives us or promises to give us something, there is an inclination to reciprocate (Perri & Brody, 2012). For example, affinity fraud offenders often contribute to their target's cause by donating money to prove their allegiance to the group with the expectation that the target audience will feel obligated to later participate in the offender's opportunity.

CASE STUDY

Consider this affinity fraud case, which involved ethnic, religious and racial affiliations.

Cambodian fraud victims reported that fellow immigrant Seng Tan, together with her husband James Bunchan, a Cambodian-born Canadian citizen, impressed many of Tan's uneducated fellow Cambodians with appearances of wealth.

Like them, Tan had fled the horrors of the Pol Pot regime in Cambodia and prayed, cried and laughed with them over their shared experiences. Bunchan gave emotional speeches to convince the immigrants to invest with him, explaining why it was their turn to prosper.

The immigrant families, who did not have enough cash to invest, collected money from relatives, cashed out retirement accounts, and took out equity loans on their homes. The loans were signed over to Bunchan and Tan, totalling more than $20 million from about 400 victims.

Tan told them they would need to pay $26,347.86 into a company called Worldwide Marketing Direct Selling, Inc., a vitamin and beauty-aid supplier. For that investment, the company would send them a $2,497 bonus, then $300 a month for life as well as money for their children. For every five investors they recruited, the payments would jump again.

Tan targeted longstanding members of the community knowing that once they bought into the investment scheme, other Cambodians would follow. Between 2000 and 2005, the investments brought returns and cheques arrived every month, just as promised.

However, after five years, the payments stopped, the Ponzi scheme collapsed, and the community lost all of its investment. The pyramid scheme and the huge losses took even leaders of the Cambodian community by surprise.

Tan, knowing the immigrant investors were wary of those outside their tight-knit community, succeeded in keeping word of their operation secret. It was only when one of the investors told someone at his place of work what had transpired that the Federal Bureau of Investigation became involved. Bunchan and Tan were found guilty of fraud in 2007 (Perri, 2011). ■

References

AP (2010). "Jury finds Indiana church financier guilty of fleecing investors in Ponzi scheme," Associated Press.

The *Economist* (2012, January 28). "Fleecing the flock."

Luo, X., Brody, R., Seazzu, A. and Burd, S. (2011). "Social engineering: the neglected human factor for information security management," *Information Resources Management Journal*, Vol. 24 No. 3, pp. 1-8.

Morgan, E. (2011). "Bills would crack down on affinity fraud in Utah," January 31, available at: www.deseretnews.com.

NASAA (2011). "Top investor traps," North American Securities Administrators Association.

Perri, F.S. (2011). "White collar criminals: the 'kinder, gentler' offender?" *The Journal of Investigative Psychology and Offender Profiling*, Vol. 8 No. 3, pp. 217-41.

Perri, F.S. & Brody, R.G. (2013). "Affinity is Only Skin Deep: Insidious Fraud of Familiarity," *Fraud Magazine*, 28(2), 42-48.

Perri, F.S. & Brody, R.G. (2012). "The Optics of Fraud: Affiliations that Enhance Offender Credibility," *Journal of Financial Crime* 1993, 305-320.

Wilson, C. (2010). "Indiana church financier faces Ponzi scheme trial," available at: http://theworldlink.com.

just THE FACTS

ILLEGAL GAMBLING

In the past, illegal gambling has been associated with images of mobsters, piles of cash and retribution for those who don't pay up. But as the illicit business goes online and technology makes it more accessible, it's drawing in more players from outside organized crime networks.

Before 1970, most forms of gambling were illegal in Canada. The *Criminal Code* was amended in 1970 to legalize certain activities and, in 1985, provinces and territories were given jurisdiction over their own lotteries, slot machines and charitable gambling activities.

In Canada, an individual can be charged under Section 201 and/or 202 of the *Criminal Code* if he or she organizes a gambling event in a common betting house (where people bet amongst themselves or the host) or common gaming house (where betting games are hosted), or is found to be an organizer of illegal gaming events. The online version of this — a gambling service — is also illegal.

The legality of gambling varies across the globe, but most illegal gambling involves games that are otherwise legal, but are being operated in illegal venues. This can include video poker machines, card or dice games and betting on sports teams. Generally, if a game is not licensed or run by a government, it is considered illegal.

Operating a sports betting scheme is banned in India and illegal in most of the United States. This draws people to do it illegally. Illegal sports betting also offers better odds for a game and therefore a better payout for a win.

In February 2013, Ontario police seized more than $2 million in 10 separate raids on users of the illegal Internet sports gambling site, Platinum Sports Book. Nineteen people in total were charged.

One of the raids was in Markham, Ont., where six people were arrested at a Super Bowl party. Charges related to bookmaking, participating or contributing to the activity of a criminal organization and keeping a common betting house. High-ranking members of organized crime groups, such as outlaw motorcycle gangs, were the targets.

In the past, law enforcement has had trouble cracking down on these types of illegal sports gambling groups because of their secretive, pyramid-style hierarchy. Gamblers place bets with bookies, who get the odds of the game from those above them. These people get their information from those even higher in the chain. This way, it is extremely difficult for bookies to know who works two rungs above them, and it is even more difficult for police to connect the dots.

In England, the illegal sports betting industry is estimated to be worth $500 billion a year. The British Broadcasting Corp. compares that to 50 times the annual profit of Toyota — the world's largest car manufacturer.

Sports gambling is starting to change the face of the game. In a recent investigation, Europol found that 680 football matches played around the world were fixed by organized crime groups. More than 400 match officials, players and criminals were suspected of being involved.

Online gambling is illegal in the United States and in many other countries across the globe. However, it's a hard crime to prosecute because website operators are based in other countries where online gambling is legal, such as Australia, France and some provinces in Canada.

Although the winnings can be big, illegal gambling hurts. It can cost federal governments hundreds of millions of dollars in lost tax revenue, encourage under-age youth to participate online and feed money to organized crime groups.

For organized crime networks, illegal gambling is a main source of income.

Between 1999 and 2002, at least eight murders occurred in Toronto that were related to illegal gambling among organized crime groups.

In 2004, Louise Russo was paralyzed from the waist down after she was shot during a botched mob hit at a sandwich shop in California. The shooter was aiming for a notorious Sicilian mafia figure who owed him money on a gambling debt.

In 2002, the Canadian Security Intelligence Service (CSIS) identified three transnational crimes as growing risks to national security — money laundering, drug trafficking and illegal gambling.

BENEATH THE SURFACE

POLICE DISMANTLE AFRICAN CHILD LABOUR OPERATION

By Mallory Procunier

Human trafficking is a transnational crime that often goes unnoticed. And in places like Burkina Faso — a landlocked country in western Africa — child labour operations can be a normal part of life.

"In these countries, things like this have been happening for years," says Sgt. Marie-Claude (M-C) Arsenault, who leads the Human Trafficking National Co-ordination Centre at the RCMP's national headquarters in Ottawa. "Some members of the community believe that children should start working young and that it's not human trafficking."

But as a member of INTERPOL's Task Force on Human Trafficking, Arsenault felt that she needed to become part of the solution. In October 2012, she travelled to Burkina Faso to teach local law enforcement members about human trafficking and prepare them to rescue almost 400 children from a dangerous gold mining operation.

RCMP

Sgt. Marie-Claude Arsenault sits with children who were rescued from a dangerous gold mining operation.

SOLID FOUNDATION

On the first day of training, Arsenault stood in front of more than 100 officials from the country's national police, gendarmerie, customs and forestry services and talked about human trafficking. Along with local instructors, she spoke about what the crime is, how to investigate it and how to approach a victim, giving officials an educational foundation to prepare them to combat human trafficking in the future.

"They have to understand the crime in order to be able to investigate it, rescue the children, interview the children and gather the evidence necessary to deliver the charges," Arsenault says.

And while she spoke to the small classroom filled with eager listeners, Arsenault couldn't help but notice how keen everyone was to learn about human trafficking.

"It was 6:00 at night, it was dark, it was hot, and they were still asking questions to the instructors," says Arsenault.

After three days of intense training, the operation began that would not only rescue hundreds of children, but would also serve as a practical application of the skills the officers had just learned.

"The philosophy behind the INTERPOL task force is to make sure the participants use these new skills and that we help them put them into use," says Arsenault. "There aren't too many organizations that do that, in terms of capacity building, to make sure they actually use the skills."

Once they were briefed, officers piled into the backs of trucks and drove to the mines, where children as young as seven were being forced to work in 70-metre deep mining holes. Traffickers would lower children into these airless, narrow holes where they would work from dusk until dawn. Their only source of oxygen was from a tube-like plastic bag, fed into the hole by a person who was fanning air down from the surface.

At four different sites, officers raided the operations, arresting traffickers and rescuing children under the age of 18. They were brought to a temporary shelter, where Arsenault waited to help.

"I saw all these children being rescued but I still knew that there were hundreds of others still out there, so I had mixed emotions," Arsenault says.

JOINING FORCES

Hakan Erdal, the co-ordinator of INTERPOL's smuggling and trafficking unit for the Trafficking in Human Beings Sub-Directorate in Lyon, France, says that when international law enforcement agencies come together like this, up-to-date information is exchanged and partners can share their expertise.

"The operation in Burkina Faso was one of the biggest operations that we have done, and we have updated our operational concept with valuable contributions from M-C," adds Erdal.

The operation was also a way to teach local law enforcement about how to dismantle human trafficking operations in the future, and educate parents and community members about how to prevent them in the first place.

Commissioner Sere Idrissa, head of INTERPOL's National Central Bureau in Ouagadougou, Burkina Faso, says that after the rescue, Arsenault took the time to educate the rescued children's parents about the need to put their children in school and keep them away from these kinds of labour operations.

"The fight against child trafficking is a daily struggle, but these operations are a way to educate and train people to better care for their children," Idrissa says. ■

Moncton Healthy Driver Research Group

The Healthy Driver Research Group uses driving simulators to test reaction times and other cognitive performance measures following a night shift.

FATIGUE AND SHIFT WORK

SMALL CHANGES CAN IMPROVE HEALTH, SAFETY

By Kristine Beaulieu, BSc (Nutr.), RD, Natasha McLaughlin-Chaisson, BSc (Nutr.), RD, Stephanie Ward, BSc (Nutr.), RD, RCMP Cpl. Dave Ward (ret.'d), and Michel Johnson, PhD, Moncton Healthy Driver Research Group, Université de Moncton

Fatigue is a major problem for shift workers due to sleep disruptions and deprivations resulting from their irregular schedules. Night workers in particular experience reduced and disrupted daytime sleep because of surrounding noise and light, domestic commitments such as childcare and meals, and because of the body's natural sleep cycle.

These recurring interruptions shorten the deep-sleep period needed to recover from physical fatigue. Over time, sleep disruptions can lead to chronic fatigue, chronic anxiety and depression.

Fatigue also has a negative effect on physical and mental task performance. Even partial sleep deprivation can cause longer (slower) reaction times. And the sleep cycle generally fails to adapt successfully to daytime sleep and night work.

Many adverse health-related problems have been reported in shift workers. Since shift workers must change their meal times, their eating habits, sleep-cycle phases and digestive functions are all disrupted. Between 20 and 70 per cent of shift workers end up with gastrointestinal problems such as disturbances in appetite, constipation, indigestion, heartburn, abdominal pains, grumbling and flatulence.

Studies of shift and night workers also report a higher prevalence of gastrointestinal disorders, such as peptic ulcers and colitis. These problems are worsened by poor food choices (eating more prepackaged food), short work breaks, nibbling, snacking rather than eating full meals and relying on stimulants, such as coffee, tea and sometimes tobacco.

Type 2 diabetes and cardiovascular disease are also more prevalent in those who work shifts. Eating at night has shown to increase the LDL/HDL cholesterol ratio. A Swedish survey found that shift workers often had more problems with obesity, high triglycerides and a low concentration of HDL (good) cholesterol compared to day workers.

According to a recent study, fatigue impairs many skills and functions. Fatigue results in poorer accuracy and timing, difficulty multi-tasking, inconsistent performance, negative attitude and mood, an impaired ability to reason, reduced situational awareness, and involuntary and uncontrollable lapses into sleep.

Employees working irregular shifts are twice as likely to be involved in a sleep-related accident and for night-shift workers, the risk is six times higher.

COUNTER-MEASURES

Although there's no quick fix to replace lost or disrupted sleep, there are counter-measures that can help, if applied appropriately.

Caffeine is a widely used stimulant that results in increased subjective energy and alertness. In night workers, low doses of caffeine (150 to 400 milligrams or 1 to 2 medium coffees) have demonstrated positive effects on performance and alertness with a decrease in sleepiness.

Researchers Reyner and Horne found that the combined treatment of caffeine and a nap was clearly superior to caffeine alone.

However, higher doses of caffeine (more than 500 milligrams or more than 3 medium coffees) appear to cause a decline in performance. Side effects of caffeine intoxication include nervousness, anxiety, restlessness, insomnia, gastrointestinal upset, tremors, increased heart rate and, in rare cases, death.

Functional energy drinks contain not only caffeine but other active ingredients such

as sugar. Glucose, a type of sugar, can have an alerting effect, but this is usually of short duration (approximately 10 minutes).

One study found that a 250-ml energy drink containing 80 milligrams of caffeine notably improved driving performance in sleep-deprived men. However, the amount of caffeine in functional energy drinks ranges from 80 milligrams to more than than 500 milligrams per bottle or can.

NAPPING

Naps can significantly reduce shift-work fatigue problems. Naps of a few hours during the night shift are important for the health and safety of shift workers. They help alleviate fatigue and sleepiness, compensate for sleep loss and decrease blood pressure and heart rate.

In addition, some studies have reported an improvement in mental performance following a nap, noting improved alertness, performance, reaction time, vigilance, memory, cognition, driving simulator performance and performance at the end of the shift.

Confusion, grogginess and cognitive performance impairment may be associated with this transition from longer naps to becoming fully awake, which can make the benefits of longer naps apparent only two to four hours after that nap. To avoid these side effects, naps should not be longer than 20 to 30 minutes. These short naps should not be taken during early morning hours or after long waking times. Naps just before the night shift should be as long as possible.

A study of Italian police drivers found that those who didn't take naps before their night shifts had an almost 40 per cent increase in accident risk compared to those who did. Arne Lowden and colleagues recommend eating breakfast before day sleep to avoid being awakened by hunger.

Physical activity can help with reducing the negative health-related effects of shift work. Shift workers who are involved in regular physical activity may be better able to tolerate the demands and strains of shift work and are generally healthier.

Exercise may be advantageous to shift workers by facilitating and promoting sleep and improving its quality. In addition, physical activity brings about a decrease in the general feeling of fatigue and an increase in vigour, alertness, resilience, hardiness and perceived energy.

For instance, one study found that 10 minutes of moderate exercise every two hours throughout a 40-hour sleep deprivation period resulted in less subjective sleepiness in individuals for up to 30 minutes after exercising, but no differences in objective performance.

Mikko Harma suggests that shift workers focus on doing some light to moderate physical exercise during their shift rather than moderate to high intensity exercise. Studies have shown that higher intensity activity can result in increased levels of fatigue and exhaustion.

Feelings of fatigue, sleepiness and other short-term effects of working unusual hours may be diminished by appropriately timed exercise.

MEALS AND SNACKS

Sleep cycle disruption may be minimized by keeping the same meal times across the shift cycle and by restricting energy intake between midnight and 6 a.m. Food choices should be varied and include complete meals and high-quality snacks. Convenience foods, high-carbohydrate foods, sugar-rich products and non- or low-fibre carbohydrate foods should be avoided.

Though the relationship between food, sleepiness and performance isn't fully understood, studies show that larger meals produce more frequent lapses of attention, a decrease in alertness and an increase in signs of sleepiness.

Spring and colleagues compared the effects of a high-protein meal (86 per cent protein) with those of a high-carbohydrate meal (80 per cent carbohydrates) on mood and performance. After the high-carbohydrate meal, women reported feeling sleepier and less vigorous. After the high-protein meal, subjects who were 40 or older reported greater tension and feeling less calm. However, there were no effects or interactions of either meal on reaction time.

Another study compared low-fat-high-carbohydrate lunches (LFHC, 29 per cent fat and 59 per cent carbs) with medium-fat-medium-carbohydrate lunches (MFMC, 45 per cent fat and 42 per cent carbs) and high-fat-low-carbohydrate lunches (HFLC, 62 per cent fat and 24 per cent carbs).

This study found that both LFHC and HFLC lunches increased the feelings of drowsiness and increased reaction times compared to the MFMC meal. Heather Love and colleagues also tested a MFMC (46 per cent fat and 42 per cent carbs) meal during a night shift and found faster reaction times compared to baseline.

TIPS FOR STAYING ALERT DURING A NIGHT SHIFT

- Take a one- to five-hour nap before your shift
- Take short naps of 20-30 minutes when possible
- Avoid exercising intensely
- Do 10-minute sessions of light to moderate exercise (eg. walk around your vehicle) when possible
- Avoid high-fat and high-carbohydrate snacks and meals
- Include a source of protein in every meal and snack, such as reduced-fat cheese, low-fat cottage cheese, fat-free Greek-style yogurt or almonds. ■

References

Alford, C.A. "Sleepiness, countermeasures and the risk of motor vehicle accidents." In: Verster J.C., Pandi-Perumal S.R., Ramaekers J.G. and de Gier J., eds. (2009). Drugs, Driving and Traffic Safety. Basel: Birkhäuser pp. 207–232

Atkinson, G. and Davenne, D. (2007). "Relationships between sleep, physical activity and human health." *Physiology & Behavior*, 90(2–3):229–35.

Costa, G. (1996). "The impact of shift and night work on health." *Applied Ergonomics*, 27(1):9–16.

Ficca, G., Axelsson, J., Mollicone, D.J., Muto V. and Vitiello, M.V. (1996). "Naps, cognition and performance." *Sleep Medicine Reviews*, 14(4):249–58.

Lloyd, H. M., Green, M. W. and Rogers, P. J. (1994). "Mood and cognitive performance effects of isocaloric lunches differing in fat and carbohydrate content." *Physiology & Behavior*, 56(1): 51–57.

Reyner, L.A. and Horne, J.A. (1997) "Suppression of sleepiness in drivers: combination of caffeine with a short nap." *Psychophysiology*, 34(6):721–5

Spring, B., Maller, O., Wurtman, J., Digman, L. and Cozolino, L. (1983). "Effects of protein and carbohydrate meals on mood and performance: interactions with sex and age." *Journal of Psychiatric Research*, 17(2):155–67.

For other key references, please contact the Moncton Healthy Driver Research Group.

CYBERBULLYING AND SEXTING

LAW ENFORCEMENT PERCEPTIONS

By Justin W. Patchin, PhD, Joseph A. Schafer, PhD, and Sameer Hinduja, PhD

Law enforcement officers often struggle to determine their proper role in addressing bullying behaviour.

Emerging social networking and other communication tools and their accompanying roles in the shift in youth behaviour complicate the situation. Historically, bullying occurred within or in close proximity to a school or neighbourhood, but technology allows present-day bullies to extend their reach.

GROWING PROBLEM

Cyberbullying includes sending threatening texts, posting or distributing libellous or harassing messages, and uploading or distributing hateful or humiliating images or videos to harm someone else. The number of American youth who experience cyberbullying ranges from five to 72 per cent, depending on the age of the group and the definition of cyberbullying.

Sexting is another issue that poses a public concern. Sexting involves sending or receiving sexually explicit or sexually suggestive nude or semi-nude images or video, generally via cellphone. Often teens initially send these images to romantic partners or interests, but the pictures can find their way to others.

Estimates of the number of youth who have participated in sexting range from four to 31 per cent. In 2010, surveys from 4,400 U.S. middle and high school students indicated that eight per cent had sent naked or semi-nude images of themselves to others, and 13 per cent reported receiving such pictures from classmates.

Cyberbullying and sexting are significant problems facing teens and schools because of the psychological, emotional, behavioural, and physical repercussions that can stem from victimization. School administrators recognize the severity of these issues, and promising practices provide these educators with what they need to know about cyberbullying and sexting, their prevention and the proper responses when incidents arise. Questions about law enforcement's role linger and deserve an answer.

SURVEY

Law enforcement officers, especially those assigned to school settings, likely will encounter cyberbullying, sexting and other forms of online impropriety. The authors collected two separate samples for their investigation of these problems.

The first, taken in May 2010, involved 336 school resource officers (SROs) who completed an online survey about cyberbullying and sexting.

The second sample included law enforcement leaders attending the FBI National Academy (FBINA), a 10-week residential career development experience at the FBI Academy in Quantico, Virginia. The authors collected data from surveys administered to 643 officers from three FBINA classes in 2010 and 2011.

Both groups responded to comparable surveys on their experiences with cyberbullying and sexting cases, as well as perceptions of their primary professional role in preventing and responding to such incidents.

Ninety-four per cent of SROs agreed that cyberbullying was a serious problem warranting a law enforcement response. Seventy-eight per cent stated that they had conducted cyberbullying investigations (an average of 16 separate incidents) during the previous school year.

Of the 336 respondents, 93 per cent indicated that sexting was an important concern for law enforcement officers. Sixty-seven per cent reported investigating an average of five sexting incidents in the previous year.

Officers reported that most cyberbullying occurred through social networking or text messaging.

One officer described an incident that involved female students spreading defamatory information about one classmate's sexual activities, choice of boyfriends and other associations.

Officers, school administrators and parents worked together to alleviate the problem by advising the students that their behaviour could be criminal and that subsequent harassment would involve the court system.

Generally, sexting incidents involve romantic partners. Images sent and received as part of a consensual relationship received informal handling with officers talking to students and parents about the seriousness of the situation. When coercion or unauthorized distribution occurred, formal

prosecution was likely.

Eighty-two per cent of the FBINA respondents recognized that cyberbullying was a significant issue requiring police involvement.

Ten per cent of the officers indicated that they had experience investigating cyberbullying cases, averaging two cases during the previous school year. While 78 per cent of the FBINA respondents determined that sexting was a considerable concern for law enforcement, only seven per cent reported that they investigated sexting incidents.

RESEARCH FINDINGS

Using hypothetical cyberbullying scenarios, all respondents rated the extent to which law enforcement should play a significant role.

They perceived the greatest role in situations involving a threat of physical harm.

For example, they used a scale with zero being no role and 10 being a significant role to rate the appropriate responsibility of officers in the following situation: A male student received an email from an unknown person threatening to kill him at school the next day. The average rating was 9.1 for the SROs and 8.6 for the FBINA respondents.

Participants indicated that a formal law enforcement response wasn't essential in situations involving potential violations of student codes of conduct. They rated the following scenario: A teacher confiscates a cellphone from a student in class and wants to determine if it contains any information that's in violation of school policy.

SROs rated the law enforcement role on average as 2.4, and FBINA respondents reported 1.4.

Law enforcement officers understand their role more clearly when the behaviour is an obvious violation of state or local law and less if there is no immediate safety concern.

Officers who recently investigated a cyberbullying or sexting case were more likely to view these issues as a significant law enforcement concern. This finding explains why SROs reported a greater law enforcement role than the FBINA respondents in all of the scenarios. SROs had direct experience with cyberbullying and sexting.

The research indicated that more young people will encounter a cyberbully than be groomed, abducted and assaulted by a stranger on the Internet.

However, over 80 per cent of study participants indicated that they needed additional training on preventing and responding to cyberbullying.

Twenty-five per cent of the SROs and over 40 per cent of the FBINA officers surveyed did not know if their state had a law specific to cyberbullying.

CONCLUSION

Law enforcement officers, especially those assigned to schools, will need to address cyberbullying at some point during their tenure. Even if the cyberbullying behaviour isn't at a criminal level, officers should handle the situation in a way that's appropriate for the circumstances.

A discussion of the legal issues may be enough to deter some first-time bullies from future misbehaviour. Officers should talk to parents about their child's conduct and the seriousness of online harassment.

Law enforcement's response will vary based on how the case was discovered, what harm has occurred, how evidence was collected, who was involved, and what level of training officers have received.

Some participants perceived that when these issues occurred away from school, the school could not take any action.

One school resource officer stated, "The incident began on Facebook and was done outside of school hours, so the school was unable to do anything about the cyberbullying."

It's important that officers understand that schools can discipline students for their off-campus behaviour when it infringes on the rights of other students or results in or has a foreseeable likelihood of causing substantial and material disruption of the learning environment of the school.

Even when the behaviour doesn't violate the law, schools can and should apply appropriate discipline. Law enforcement officers play an important role in ensuring that proper responses are provided to minimize the future risk and harm that cyberbullying and sexting may create. ■

Dr. Patchin is an associate professor of criminal justice at the University of Wisconsin, Eau Claire.

Dr. Schafer is a professor and chair of the Department of Criminology and Criminal Justice at Southern Illinois University, Carbondale.

Dr. Hinduja is an associate professor in the School of Criminology and Criminal Justice at Florida Atlantic University.

This article excerpt is reprinted courtesy of the FBI *Law Enforcement Bulletin*. To view the full article, visit: www.fbi.gov.

POLICE PERCEPTIONS REGARDING RESPONSIBILITY IN DEALING WITH CYBERBULLYING

With 0 being no law enforcement role or responsibility and 10 being a very important or significant role or responsibility, to what degree should law enforcement be involved?	School Resource Officers	FBI National Academy
A male student receives an email from an unknown person threatening to kill him at school tomorrow.	9.1	8.6
A parent calls to report that her son has a naked image of a female student from his school on his cellphone.	8.3	6.3
A parent calls the police department to report that her son is being cyberbullied by another youth in their neighborhood.	7.8	6.5
A male student reveals another classmate's sexual orientation (without permission) via Twitter to the rest of the student body.	5.7	4.0
A female student receives a text message from another classmate calling her a slut.	4.2	3.4
A teacher confiscates a cell phone from a student in class and wants to determine if it contains any information that violates school policy.	2.4	1.4

A FLASH OF REALITY

TORONTO COP SPOTLIGHTS MENTAL HEALTH IN TV DRAMA

Cst. Calum de Hartog has worked at the Toronto Police Service for 13 years but has been making films since his youth. Now, de Hartog is blending both aspects of his life after creating a new CBC series, Cracked *— a procedural drama based on the force's pairing of psychiatric nurses with police officers in the field. He spoke to* Gazette *writer Mallory Procunier about his choice to highlight mental health.*

Russ Martin

Cst. Calum de Hartog of the Toronto Police Service is the creator of *Cracked* — a procedural police drama focused on mental health.

AS PART OF THE EMERGENCY TASK FORCE, YOU'VE HAD A LOT OF POLICING EXPERIENCE THAT COULD MAKE GREAT TELEVISION. WHY FOCUS ON MENTAL HEALTH?

That was a pretty organic choice that evolved basically from our crisis intervention team that I've interacted with on my days on patrol and also as a negotiator. The worlds collided and I took it from there. We created more of an investigative unit than anything else.

WHAT'S THE GOAL OF THE SHOW?

To make an engaging, exciting, character-driven series that could shine a light on a very street-level view of not only what it's like as a first responder but also how these people navigate the world of emotionally disturbed persons and mental health issues. It's storytelling, so it's not really trying to educate people as much as it's trying create an exciting dialogue around a subject matter that can sometimes get lost in the shuffle.

HOW MUCH OF THE SHOW IS BASED ON YOUR EXPERIENCES?

It's more bits and pieces and situations you find yourself in, and people you meet along the way. Little bits of each of those things sort of weave their way into the fabric of a storyline or even a character. I'm also working with a team of writers so everybody brings their own experiences to it and sort of threads them into various storylines that have been decided earlier on.

HOW DO YOU STRADDLE THE LINE BETWEEN SENSATIONAL TELEVISION AND SHARING THE REALITIES OF THE FIELD?

It's a delicate balance. We're not making a documentary, but we have certain areas and themes we want to touch on in an episode. The biggest learning curve for me was figuring out the structure of what goes into an episode of television. You want to make things compelling and engaging and scary and sad and exciting all at the same time. You're taking in a lot of requirements to make for an engaging hour-long drama and you're sort of stretching a lot of the situations.

HOW HAVE YOUR COLLEAGUES REACTED?

They love it! They're super supportive and they just get a kick out of it as much as I do. I've also gotten some incredible feedback from police officers across the country just saying that they found it really interesting. I heard it opened up some creative outlets for them. Whether it's photography, movies or writing, all those things seem to be a neat enjoyment that people are getting out of it.

IS IT IMPORTANT FOR POLICE OFFICERS TO HAVE A HOBBY ON THE SIDE?

I think it's important to have something on the side that you really love to do. In a lot of cases it's family, hobbies or sports, but a life outside of policing I find is incredibly useful in trying to live a life of balance. I also run a film mentoring program with inner-city kids called the City Life Film Project and that's been incredibly successful over the years. Ultimately, it's a six-month-long workshop and at the end of it, the kids make a short, professional-grade film with some of the best in the business. We then have a big screening event and that's after they've pitched the film so they've gone through the process of what it's like and they have an idea how to develop it and pitch it and then make it. Creativity and art has been a really great bridge in creating dialogue between people and that's just the voice I've chosen to articulate with. ■

MIND OVER MATTER

MEMBER, ACADEMIC REACH OUT

By Sigrid Forberg

It was a chance encounter that brought Cst. Joanne Koole's attention to Professor Adrian Owen's research on individuals in vegetative states.

At a medical symposium in Vancouver, British Columbia (B.C.), Koole sat in on a lecture Owen delivered about his research using brain imaging to communicate with people who are otherwise unable to express themselves.

As it turns out, according to Owen's research, approximately one in five individuals who are unresponsive physically are still conscious inside but unable to express that. He's been able to communicate with them by running them through an MRI machine and asking them yes or no questions that would light up different areas of the brain.

"I was just sitting there, thinking, 'oh man, why don't we use this for investigations'?" says Koole. "I was just so excited but I thought, 'of course they've thought of this, I shouldn't even say anything because it's so obvious.' "

BRIGHT IDEAS

Koole, who was a coroner before joining the RCMP, was thinking about the possibility of collecting statements through Owen's process of the unsolved cases that left victims of gunshot wounds, asphyxiation, forced near drowning or blunt force trauma in what appear to be vegetative or unresponsive states.

To her great surprise, when she spoke to Owen after the lecture, she discovered he hadn't previously thought of applying his research in a policing context. But he was enthusiastic and interested in pursuing it.

Koole wrote up a decision document and with the encouragement of her manager in Burnaby, B.C., pursued the idea. When she transferred to the Provincial Intelligence Centre of B.C., S/Sgt. Baltej Dhillon, a polygraph expert, encouraged her and helped her move the idea up the ranks as well as reassured her that although it might only meet the needs of a very few, the project would still have value.

"We work in service of the people of this country and if there's a technique we may only use once every five years but can potentially further investigations, then it should absolutely be a part of our thinking processes and investigative toolbox," says Dhillon.

And the idea was met with enthusiasm all the way up the chain of command. Now the national project co-ordinator for vegetative state victims, Koole is now working on tracking down the right victims for Owen to communicate with. She explains it's almost like a perfect storm to find a person who fits all the criteria.

"There's not many victims in this state," says Koole. "Many have died over the years or their cases have been solved. But to find that one person and to bring some peace to their families, that would be incredible. That's what I'm hoping for."

LIMITLESS POSSIBILITES

When Koole approached him, Owen had been using his research in a purely clinical context for 15 years. On a research grant from the Canadian government, he's been working at Western University in London, Ont., for the past two and a half years. He says that while this project was never part of his initial plans, he says he finds it a beautiful application of his work.

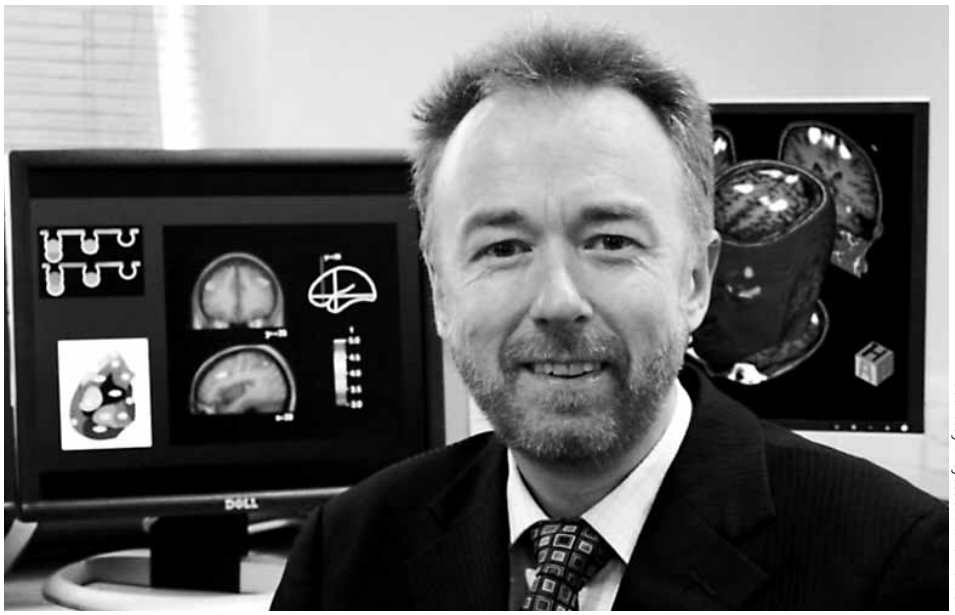
"I've always been interested in finding applications for the techniques and science that we do," says Owen. "This is a completely natural extension of that. To see what I've worked on for 15 years applied to a real world situation is incredibly satisfying."

It may be a while before Koole and Owen find the right victim and collecting statements from a person diagnosed as in a vegetative state is unlikely to hold up as evidence in court, but the goal is just to generate leads that can help move a case along for investigators, who will then rely on traditional techniques to solve it.

As it stands now, the only thing standing in the way of further progress is finding that perfect person. Dhillon says he was happy to see the support and encouragement Koole's enthusiasm received. He adds he thinks that's the way it should always be in the force.

"My fear as a manager is that other Joanne Kooles out there in our organization have ideas that don't make it past their managers," says Dhillon. "I would encourage young members to always look for new ideas to help us keep up with the times and meet our first requirement as police officers, which is to create safe communities." ■

Professor Adrian Owen uses brain imaging in an attempt to communicate with people in vegetative states.



Courtesy Professor Adrian Owen

LATEST RESEARCH IN LAW ENFORCEMENT

Sworn members of seven law enforcement agencies in the United States were polled about police training. The single highest-rated topic was firearms training.

The following are excerpts from recent research related to justice and law enforcement and reflect the views and opinions of the authors and not necessarily those of the organizations for which they work. To access the full reports, please visit the website links at the bottom of each summary.

INTIMATE PARTNER VIOLENCE RISK ASSESSMENT TOOLS: A REVIEW

By Melissa Northcott

The criminal justice system is faced with the task of protecting victims of intimate partner violence, while at the same time ensuring that the rights of the accused are not violated. This tension is evident at different stages in the criminal justice system process such as at bail, sentencing and parole.

One approach that's been adopted to manage the above-noted issues is assessing the risk that offenders pose for re-offending and how to best manage these offenders. Specialized risk assessment tools have been created for these purposes and are being used in many jurisdictions.

RISK ASSESSMENT TOOLS

Some risk assessments focus on the offender, while others are focused on the victim and the risk that they will be revictimized. This report discusses the general use of intimate partner violence risk assessment tools, but focuses more strongly on the use of risk assessment tools as they are used for the purposes of violence prediction.

The majority of risk assessment tools used in criminal justice settings were originally developed by forensic mental health professionals to be used in forensic mental health settings. They're now not only being used in a number of different settings, but their use in other forensic areas is growing.

Types of intimate partner violence risk assessment tools:

Unstructured clinical judgment — A professional collects information and renders a risk assessment based on his or her own subjective judgment.

Structured clinical judgment — Assessors follow a set of guidelines that include specific risk factors that should be considered. These risk factors are determined based on theoretical and general empirical support.

Actuarial approach — Based on the use of predictive or risk factors from specific empirical research. These risk factors are assigned a numerical value and a total score is generated through an algorithm and then used to estimate the probability that the individual will re-offend within a specific time period.

OTHER APPROACHES

There are other methods and tools used for the purposes of predicting intimate partner violence recidivism. These methods include consulting the victim on their prediction of the offender's likelihood of recidivism and the use of other risk assessment tools designed to predict general and violent offending.

CONCLUSION

There are a number of factors that the assessor must consider when choosing a tool or an approach, including their own role, the population they are assessing and the purpose of the assessment. It's also important for the assessor to keep in mind the various strengths and limitations of the specific risk assessment tools and of risk assessment tools more generally. Keeping these elements in mind, it's possible for an assessor to choose the most appropriate tool to guide the assessment of the risk that an offender poses to an intimate partner.

TO ACCESS THE FULL REPORT, PLEASE VISIT:
WWW.JUSTICE.GC.CA

EFFECTIVE COMMUNITY-BASED SUPERVISION OF YOUNG OFFENDERS

By Chris Trotter

A lot has been written about what works in interventions with offenders. In recent years, there have also been a small number of studies focusing on what works in the routine supervision of offenders on probation, parole or other community-based orders.

These studies have found that certain

supervision skills offered by supervisors can lead to reduced levels of reoffending. These studies have been predominantly undertaken with adult offenders.

This paper describes a study that examined the relationship between the use of these practice skills by supervisors in juvenile justice in New South Wales and reoffending rates by their clients (those under their supervision). It was hypothesized that it would be possible to identify the extent to which supervisors used particular practice skills through the direct observation of interviews by trained research officers. It was also hypothesized that the more the effective practice skills highlighted in earlier research were used, the less frequently the offenders under supervision would reoffend.

SAMPLE

This study was undertaken in the Department of Juvenile Justice in New South Wales. Community-based supervision represents the primary form of intervention with young offenders in New South Wales, as well as throughout Australia.

In Australia, in 2008-09, around 7,200 young people were under juvenile justice supervision on any given day. Most (90 per cent) were under community-based supervision, with the remainder in detention. In 2009-10, 4,251 young offenders were under the supervision of the NSW Department of Juvenile Justice on community-based orders.

After receiving university and NSW Department of Juvenile Justice ethics approval, juvenile justice staff with responsibility for direct supervision of young offenders were invited to be involved in the project. Forty-eight staff members initially volunteered. For each worker, the next five clients allocated to them became eligible for the study.

Interviews between the staff members and young people were then observed within three months of the young person receiving their court order. In total, 117 interviews were observed, conducted by 46 workers over a period of four years; 39 in a pilot project and the remainder as part of a project funded through a Criminology Research Council grant.

DISCUSSION

One study also found that supervisors who had completed social work and welfare qualifications (courses in which these skills are commonly taught) were more likely to use the skills and more likely to have clients with lower recidivism.

These findings have implications for selection, training and the roles of youth justice staff. There is potential for widespread reductions in recidivism if juvenile justice organizations prescribe a counselling role to supervisors and employ staff with relevant qualifications. Ongoing training and supervision focused on effective practice skills may provide for further reductions in reoffending. The benefits are likely to be further increased by regular observation and analysis of interviews between juvenile justice workers and their supervisors, and with feedback, discussion and coaching in order to provide for ongoing skill development.

TO ACCESS THE FULL REPORT, PLEASE VISIT:
WWW.AIC.GOV.AU

POLICE TRAINING

By Gary Cordner, Jack McDevitt and Dennis Rosenbaum

This report from the National Police Research Platform summarizes responses from the first round of organizational surveys conducted in 2010 and early 2011, focusing on police training.

Specifically, respondents were asked to rate the in-service/post-academy training they had received during their careers in regard to how well that training had prepared them to do their jobs as police officers. Additionally, supervisors were asked to rate the formal supervisory training they had received.

METHODS

The training survey was administered in seven participating agencies located in seven different states — two small agencies, one medium-sized agency, two large agencies, and two very large agencies. In total, 1,056 responses were received from sworn personnel.

The survey items reported focus on respondents' assessment of the quality of the post-academy training that they have received. The survey did not attempt to measure the amount of in-service training received.

SOURCES OF TRAINING

The sharpest differences between the seven departments pertained to in-house training — officers in four of the agencies rated in-service training provided by their department highest, but in two other agencies, in-house training was rated lowest. Interestingly, these judgements didn't seem to coincide directly with agency size, as officers from both a small agency and a very large agency gave lowest ratings to in-service training provided by their own department.

TYPES OF TRAINING

Survey respondents were asked to rate the in-service/post-academy training they had received in 25 topical areas within the general categories of field training, skills, policies and procedures, dealing with special populations, community policing, and technology. Overall ratings were in the average to good range. For the entire sample of respondents, the single highest-rated training topic was firearms training while the lowest was "how to use in-car cameras." These combined results should be viewed with caution, however, because the greater number of respondents from the larger agencies tends to dominate the responses.

SUPERVISORY TRAINING

Respondents were asked if they had official responsibility as the primary supervisor of one or more full-time employees. Those answering yes were asked to evaluate the formal supervisory training they had received on 10 specific topics. Combined ratings on the 10 topics in two of the agencies (one large and one very large) were above 2.9, nearly reaching the 3.0 "good" threshold. The average ratings in the other five agencies varied between 2.2 and 2.6, in the middle range between "average" and "good."

IMPLICATIONS

The findings demonstrate a degree of unevenness in police in-service and supervisory training and the capacity of the platform surveys to detect these differences. When applied to a larger sample of agencies and officers, the training survey should provide insights about both trends and norms for agencies of different sizes and regions of the country. ■

TO ACCESS THE FULL REPORT, PLEASE VISIT:
WWW.NIJ.GOV

CLUES IN THE CREASES

PALM PRINT DATABASE HELPS CONNECT CASES

By Sigrid Forberg

The RCMP has created a new database that will help analysts search and compare palm prints left behind at crime scenes.

Until recently, the RCMP didn't have the means to compare palm prints electronically like it does fingerprints. Oftentimes palm prints would be submitted in a file along with fingerprints, but analysts would be unable to process them. Unless the investigator had a set of palm prints to manually compare against, there was no national database to search palm prints.

The RCMP is now adding those to the database and searching all of the palm prints previously submitted from historical scenes of sexual assaults, robberies and homicides, hoping to generate a hit.

"There are a lot of cases with palms that are technically still active. We're going to try everything that comes in," says Jason Ruttan, a fingerprint examiner with the RCMP.

The hope is that by searching older latent cases as well as current files as they come in, analysts will be able to help generate investigative leads in unsolved cases that range from break and enters to sexual assaults and homicides — a technique they've already found effective with fingerprints.

INCREASED INFORMATION

Palm prints share many of the unique attributes and traits like ridge endings and bifurcations that you would find in a fingerprint. Those unique aspects, known as minutiae, can be plotted out like points on a map and contrasted in the exact way analysts compare fingerprints.

And because of their comparative size, palms often offer more distinguishing features for analysts to make positive identifications.

"It's more information," says Peter Alain, a fingerprint examiner with the RCMP. "For example, with a break and enter, oftentimes the person breaking in is going to use force. And when they use force, they're probably going to use their whole hand to push open a window. Now, if we don't hit it with the fingers, we could potentially hit it with the palm prints."

The database will be populated with palm impressions submitted from 26 different police agencies across the country, which will increase as more of these prints continue to go online. Analysts and investigators are hopeful that as the database collection continues to grow, the number of matches will as well.

"The rule of thumb now is any new offenders are going to be added to our database if their palms are taken electronically," says Alain. "It's new, so it is going to take some time before we're able to generate a hit but hopefully down the road we'll be able to."

By searching older latent cases and current files using the palm print database, RCMP fingerprint analysts hope to generate investigative leads in unsolved cases.

RCMP

ON POINT

Most of the comparative work can be done through the computer. Once the analyst enters a file, a list of the most similar prints in the database will appear. Analysts compare the images side-by-side to determine if a positive identification is possible.

However, it's not as simple as letting the computer run. Analysts play an active role in making identifications. Of the approximately 30 latent examiners on staff, Alain says many have worked a decade or more in the field of fingerprint comparison and rely on their expertise and experience to draw their conclusions. Ruttan adds that things aren't always straightforward; people can behave erratically — especially at the scene of a crime.

"We can't make assumptions when we're dealing with fingerprints," says Ruttan. "Things are not always as they appear when trying to recognize information in friction ridge impressions."

Ruttan gives the example of a case in which three fingerprints were left on a book found at the scene of the crime. After analyzing the prints, he realized that they didn't appear on the object in the order they appear on the hand, which is why it's so important each print be approached individually and that the information analyzed critically.

The United States' Federal Bureau of Investigation is also in the process of developing its own palm print database, while countries like England and Wales have had established searchable systems for a couple years now. Supt. Alain Bouchard, the director of Integrated Forensic Identification Services (IFIS), adds that the palm print databases are an increasingly important tool to help fulfill an agency's policing mandate.

"We're just keeping up with the times," says Bouchard. "We're in the business of solving crimes so the idea is that the more we get, the more the database is going to be built up and the more impressions we'll have to compare."